AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT	1. CONTRACT ID CODE	PAGE 1 OF 2

2. AMENDMENT/MODIFICATION NO.	3. EFFECTIVE DATE	4. REQUISITION/PURCHASE REQ. NO.	5. PROJECT NO. (If applicable)
P00011	See Block 16C	21436776	

6. ISSUED BY	CODE 47QFCA	7. ADMINISTERED BY (If other than item 6)	CODE
GSA/FEDSIM Acquisition (QF0B1E) 1800 F Street, NW, 3100 Washington, DC 20405 Contract Specialist Name: Leverne T Frierson Contract Specialist Phone: 999-999-9999			

8. NAME AND ADDRESS OF CONTRACTOR (No., Street, County, State and ZIP Code)	(X)	9A. AMENDMENT OF SOLICITATION NO.
PERSPECTA ENTERPRISE SOLUTIONS LLC 13600 EDS DR A3S HERNDON, VA, 20171-3225 Phone: (703) 742-2365 Fax: (703) 742-2674		9B. DATED (SEE ITEM 11)
	X	10A. MODIFICATION OF CONTRACT/ORDER NO. 47QTCK18D0030 / 47QFCA20F0015
		10B. DATED (SEE ITEM 13) 12/18/2019
CODE FACILITY CODE		

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

☐ The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers ☐ is extended, ☐ is not extended.

Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods: (a) By completing items 8 and 15, and returning ____ copies of the amendment; (b) By acknowledge receipt of this amendment on each of the offer submitted; or (c) By separate letter or telegram which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGEMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPEC FIED MAY RESULT N REJECTION OF YOUR OFFER. If by virtue of this amendment your desire to change an offer already submitted, such change may be made by telegram or letter provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the opening hour and data specified.

12. ACCOUNTING AND APPROPRIATION DATA (If required)

285F.Q00FB000.AA10.25.AF151.H08 Total Amount of MOD: $15,000,000.00

13. THIS ITEM ONLY APPLIES TO MODIFICATION OF CONTRACTS/ORDERS. IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.

	A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.
	B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation date, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).
	C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:
X	D. OTHER (Specify type of modification and authority) 52.232-22 Limitation of Fund

E. IMPORTANT: Contractor ☒ is not, ☐ is required to sign this document and return ____ copies to he issuing office.

14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.)

The purpose of this modification is stated in the SF 30 Continuation Page(s). See award documents for details.

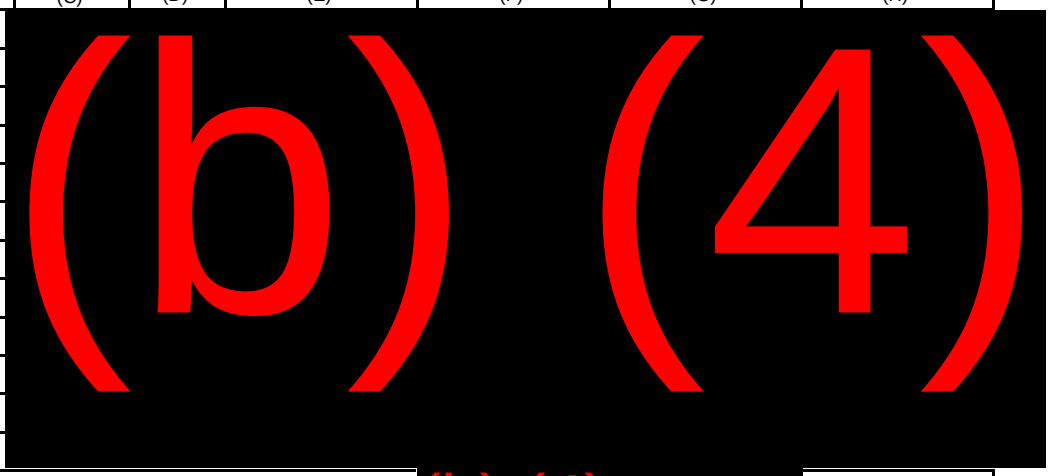
Except as provided herein, all terms and conditions of the document referenced in item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect.

15A. NAME AND TITLE OF SIGNER (Type or print)	16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print)
	Nydia Roman-Albertorio

15B. CONTRACTOR/OFFEROR	15C. DATE SIGNED	16C. DATE SIGNED
(Signature of person authorized to sign)	(b) (6)	30 Mar 2021

		PAGES

Line Item Summary							
ITEM NO. (A)	SUPPLIES OR SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	Rev. Ext. Price (F)	Prev. Ext. Price (G)	Amount Of Change (H)
0001	**Labor - Base Period**						
0001a	**Labor-CARES Act**						
0002	**Travel - Base Period**						
0003	**ODCs-Base Period**						
0004	**TOOLS-Base Period**						
0005	**CAF - Base Period**						
1001	**Labor-Option Year 1**						
1001a	**Labor-CARES Act**						
1002	**Travel-Option Year 1**						
1003	**ODCs-Option Year 1**						
1004	**TOOLS-Option Year 1**						
1005	**CAF-Option Year 1**						
				TOTALS:	(b) (4)		**$15,000,000.00**



The purpose of this modification is to: 1) Obligate to $15,000,000 in No-Year funds funding to Option 1 (OY1) Period CLIN 1001 (Labor) and CLIN 1002 (Travel).

1. Attachment B – Incremental Funding Chart is updated to reflect the obligated funding to CLIN 1001 and CLIN 1002 as follows:

    a. CLIN 1001 (Labor) total funded is increased by $14,962,000 from $18,490,841 to $33,452,841.
        i. CLIN 1001 (Labor) funded cost is increased by $13,960,997 from $17,253,747 to $31,214,744
        ii. CLIN 1001 (Labor) funded award fee is increased by $1,001,003 from $1,237,094 to $2,238,097
    b. CLIN 1002 (Travel) funding is increased by 38,000 from $82,150 to $120,150

As a result of the modification, Section B.6.1, Incremental Funding Limitation of Government's Obligation, is updated to reflect the estimated period of performance covered by the allotments for the mandatory CLINs.

Task Order total funding increased by $15,000,000 from $80,504,205 to $95,504,205.

Task Order ceiling remains unchanged at $810,580,971.

All changes are noted by the black change bars in the right margin of the conformed TO.

All other terms and conditions remain unchanged.

TASK ORDER (TO)

47QFCA-20-F-0015 Modification P00011
Consular Affairs Enterprise Infrastructure Operations (CAEIO)
in support of:
Department of State (DOS)
Bureau of Consular Affairs (CA)
Office of Consular Systems and Technology/Systems Operations Division (CST/SO)

Issued to:
Perspecta Enterprise Solutions, LLC

Awarded under the General Services Administration (GSA) *(*Alliant 2 (GWAC)*)*
Multiple Award Contracts
Conducted under Federal Acquisition Regulation (FAR) 16.505

Issued by:
The Federal Systems Integration and Management Center (FEDSIM)
1800 F Street, NW (QF0B)
Washington, D.C. 20405

December 18, 2019

FEDSIM Project Number
47QFCA-19-S-0016

B.1 GENERAL

The work shall be performed in accordance with all Sections of this Task Order (TO) and the contractor's Basic Contract, under which the resulting TO will be placed. An acronym listing to support this Task Order is included in (**Section J, Attachment A)**.

B.2 CONTRACT ACCESS FEE

The General Services Administration's (GSA) operating costs associated with the management and administration of this contract are recovered through a Contract Access Fee (CAF). In accordance with the Alliant base contract, the CAF shall be 0.75 percent of the total TO value with a cap of $100,000 per year per order (when order is in excess of $13.3M per order year). This TO shall have a separate Contract Line Item Number (CLIN) to cover this access fee, and this CAF shall be obligated at Task Order Award (TOA).

B.3 ORDER TYPES

The contractor shall perform the effort required by this TO on a Cost-Plus-Award-Fee (CPAF) basis for:

a. Mandatory Labor CLIN: 0001
b. Optional Labor CLINs (if exercised): 1001, 2001, 3001, 4001, 5001, and 6001

The Contractor shall perform the effort required by this TO on a Not-to-Exceed (NTE) basis:

a. Long-Distance Travel CLIN (if exercised): 0002, 1002, 2002, 3002, 4002, 5002, 6002
b. Optional ODCs (if exercised) CLIN(s): 0003, 1003, 2003, 3003, 4003, 5003, 6003
c. Optional Tools CLIN(s) (if exercised): 0004, 1004, 2004, 3004, 4004, 5004, 6004
d. CAF CLIN: 0005
e. Optional CAF CLINs (if exercised): 1005, 2005, 3005, 4005, 5005, 6005

B.4 SERVICES AND PRICES/COSTS

Long-distance travel is defined as travel over 50 miles from the Department of State (DOS), Consular Affairs (CA) Headquarters location at 600 19th Street, N.W., Washington, D.C. Local travel will not be reimbursed.

The following abbreviations are used in this price schedule:

CAF	Contract Access Fee
CLIN	Contract Line Item Number
CPAF	Cost-Plus-Award-Fee
NTE	Not-to-Exceed
ODC	Other Direct Cost
QTY	Quantity

B.4.1 BASE PERIOD

MANDATORY CPAF LABOR CLIN

CLIN	Description	Cost	Award Fee	Total CPAF
0001	Labor (Tasks 1–5)	(b) (4)		$58,933,096

CARES ACT REIMBURSEMENT CLIN

CLIN	Description		Total NTE Price
0001a	Labor (Tasks 1-5)	NTE	$1,094,434

COST-REIMBURSEMENT TRAVEL, TOOLS, and ODC CLINs

CLIN	Description		Total NTE Price
0002	Long-Distance Travel Including Indirect Handling Rate (b) (4)	NTE	$500,000
0003	ODCs Including Indirect Handling Rate (b) (4)	NTE	$25,000,000
0004	Tools Including Indirect Handling Rate (b) (4)	NTE	$10,000,000

MANDATORY CAF

CLIN	Description		Total Ceiling Price
0005	CAF	NTE	$100,000

TOTAL CEILING BASE PERIOD CLINs: $ 95,627,530

B.4.2 FIRST OPTION PERIOD

CPAF LABOR CLIN

CLIN	Description	Cost	Award Fee	Total CPAF
1001	Labor (Tasks 1–5)	(b) (4)		$79,958,226

CARES ACT REIMBURSEMENT CLIN

CLIN	Description		Total NTE Price
1001a	Labor (Tasks 1-5)	NTE	$800,000

COST-REIMBURSEMENT TRAVEL, TOOLS, and ODC CLINs

CLIN	Description		Total NTE Price
1002	Long-Distance Travel Including Indirect Handling Rate (b) (4)	NTE	$500,000
1003	ODCs Including Indirect Handling Rate (b) (4)	NTE	$25,000,000
1004	Tools Including Indirect Handling Rate (b) (4)	NTE	$10,000,000

CAF

CLIN	Description		Total Ceiling Price
1005	CAF	NTE	$100,000

TOTAL CEILING FIRST OPTION PERIOD CLINs: $116,358,226

B.4.3 SECOND OPTION PERIOD

CPAF LABOR CLIN

CLIN	Description	Cost	Award Fee	Total CPAF
2001	Labor (Tasks 1–5)	(b) (4)		(b) (4)

COST-REIMBURSEMENT TRAVEL, TOOLS, and ODC CLINs

CLIN	Description		Total NTE Price
2002	Long-Distance Travel Including Indirect Handling Rate (b) (4)	NTE	$500,000
2003	ODCs Including Indirect Handling Rate (b) (4)	NTE	$25,000,000
2004	Tools Including Indirect Handling Rate (b) (4)	NTE	$10,000,000

CAF

CLIN	Description		Total Ceiling Price
2005	CAF	NTE	$100,000

TOTAL CEILING SECOND OPTION PERIOD CLINs: (b) (4)

B.4.4 THIRD OPTION PERIOD

CPAF LABOR CLIN

CLIN	Description	Cost	Award Fee	Total CPAF
3001	Labor (Tasks 1–5)	(b) (4)		(b) (4)

COST-REIMBURSEMENT TRAVEL, TOOLS, and ODC CLINs

CLIN	Description		Total NTE Price
3002	Long-Distance Travel Including Indirect Handling Rate (b) (4)	NTE	$500,000
3003	ODCs Including Indirect Handling Rate (b) (4)	NTE	$25,000,000
3004	Tools Including Indirect Handling Rate (b) (4)	NTE	$10,000,000

CAF

CLIN	Description		Total Ceiling Price
3005	CAF	NTE	$100,000

TOTAL CEILING THIRD OPTION PERIOD CLINs: (b) (4)

B.4.5 FOURTH OPTION PERIOD

CPAF LABOR CLIN

CLIN	Description	Cost	Award Fee	Total CPAF
4001	Labor (Tasks 1–5)	(b) (4)		(b) (4)

COST-REIMBURSEMENT TRAVEL, TOOLS, and ODC CLINs

CLIN	Description		Total NTE Price
4002	Long-Distance Travel Including Indirect Handling Rate (b) (4)	NTE	$500,000
4003	ODCs Including Indirect Handling Rate (b) (4)	NTE	$25,000,000
4004	Tools Including Indirect Handling Rate (b) (4)	NTE	$10,000,000

CAF

CLIN	Description		Total Ceiling Price
4005	CAF	NTE	$100,000

TOTAL CEILING FOURTH OPTION PERIOD CLINs: (b) (4)

B.4.6 FIFTH OPTION PERIOD

CPAF LABOR CLIN

CLIN	Description	Cost	Award Fee	Total CPAF
5001	Labor (Tasks 1–5)	(b) (4)		(b) (4)

COST-REIMBURSEMENT TRAVEL, TOOLS, and ODC CLINs

CLIN	Description		Total NTE Price
5002	Long-Distance Travel Including Indirect Handling Rate (b) (4)	NTE	$500,000
5003	ODCs Including Indirect Handling Rate (b) (4)	NTE	$25,000,000
5004	Tools Including Indirect Handling Rate (b) (4)	NTE	$10,000,000

CAF

CLIN	Description		Total Ceiling Price
5005	CAF	NTE	$100,000

TOTAL CEILING FIFTH OPTION PERIOD CLINs: (b) (4)

B.4.7 SIXTH OPTION PERIOD

CPAF LABOR CLIN

CLIN	Description	Cost	Award Fee	Total CPAF
6001	Labor (Tasks 1–5)	(b) (4)		(b) (4)

COST-REIMBURSEMENT TRAVEL, TOOLS, and ODC CLINs

CLIN	Description		Total NTE Price
6002	Long-Distance Travel Including Indirect Handling Rate (b) (4)	NTE	$500,000
6003	ODCs Including Indirect Handling Rate (b) (4)	NTE	$25,000,000
6004	Tools Including Indirect Handling Rate (b) (4)	NTE	$10,000,000

CAF

CLIN	Description		Total Ceiling Price
6005	CAF	NTE	$100,000

TOTAL CEILING SIXTH OPTION PERIOD CLINs: (b) (4)

GRAND TOTAL CEILING ALL CLINs: **$810,580,971**

B.5 SECTION B TABLES

B.5.1 INDIRECT/ MATERIAL HANDLING RATE

Long-Distance Travel, Tools, and ODC costs incurred may be burdened with the contractor's indirect/material handling rate in accordance with the contractor's disclosed practices, provided that the basic contract does not prohibit the application of indirect rate(s) on these costs.

a. If no indirect/material handling rate is allowable in accordance with the contractor's disclosed practices, no indirect/material handling rate shall be applied to or reimbursed on these costs.
b. If no rate is specified in the schedule of prices above, no indirect rate shall be applied to or reimbursed on these costs.

The indirect handling rate over the term of the TO shall not exceed the rate specified in the schedule of prices above.

B.5.2 DIRECT LABOR RATES

Labor categories shall be mapped to existing Alliant 2 labor categories.

B.6 INCREMENTAL FUNDING

B.6.1 INCREMENTAL FUNDING LIMITATION OF GOVERNMENT'S OBLIGATION

Incremental funding in the amount of **$95,504,205** for **CLINs 0001 through 1005** is currently allotted and available for payment by the Government. Additional incremental funding for these CLINs may be allotted and available for payment by the Government as the funds become available. The estimated period of performance covered by the allotments for the mandatory CLINs is from award through **July 9, 2021**, unless otherwise noted in Section B. The TO may be modified to add funds incrementally up to the maximum of **$810,580,971** over the performance period of this TO. These allotments constitute the estimated cost for the purpose of Federal Acquisition Regulation (FAR) Clause 52.232-22, Limitation of Funds, which applies to this TO on a CLIN-by-CLIN basis.

See Section J, Attachment B - Incremental Funding Chart (Excel Spreadsheet).

B.7 AWARD FEE RESULTS REPORTING TABLE

The Award Fee Determination Plan (AFDP) establishes award fee. See **Section J, Attachment C.**

C.1 BACKGROUND AND MISSION

The Department of State's Bureau of Consular Affairs (CA) highest priority is the welfare and protection of United States (U.S.) citizens at foreign locations, supporting border security at home, and facilitating safe entry of travelers without compromising U.S security. CA issues passports to U.S. citizens, issues immigrant and non-immigrant visas to foreign nationals, and serves American citizens during life's important moments— births, deaths, disasters, and medical emergencies abroad. CA ensures responsive and efficient Consular services overseas and effective passport operations domestically.

The Office of Consular Systems Technology (CST) within the Bureau of CA is tasked with designing, installing, operating and supporting Information Technology (IT) systems and supporting infrastructure required by CA's global mission. This includes the Hardware (HW)/ Software (SW) platforms on which the CA systems reside and operate as well as providing operational support for CA applications and databases. Currently, CA applications and systems are modernized through the ConsularOne program. This TO will provide support to new and modernized applications as well as to the existing legacy infrastructure, systems, and applications, and will provide support to the infrastructure on which all CA systems reside and operate. CST plans, develops, directs, and coordinates Consular IT systems for DOS passport, visa, and overseas citizen services operations from initial concept through production. Within CST, the Service Operations Division (CST/SO) engineers, implements, and operates production hosting environments across the global CA IT enterprise, and provides support to the CA IT systems and databases. CST/SO also is responsible for ensuring effective and efficient delivery of IT services for CA including availability, recoverability, incident, and problem management, and user support through a Service Desk (SD).

Consular IT systems are installed at over 350 facilities world-wide including embassies, consulates, Consular agencies, CA Headquarters, and domestic Passport Agencies and Visa Centers. The data within the consular systems replicates to central databases housed within domestic DOS Data Centers. Over 40,000 DOS and partner Federal agency users access these systems and data on a regular basis. CA/CST is responsible for effective and efficient delivery of IT services and proactive management of the IT systems that support the mission of CA. These IT systems are critical to the timely processing of passport and visa applications with the requisite level of accuracy and security that is essential to operating in the post-9/11 environment.

C.1.1 PURPOSE

CA/CST requires contractor support to provide Operations and Maintenance (O&M) of the global CA IT environment within an Information Technology Service Management (ITSM) framework. The title of this effort is Consular Affairs Enterprise Infrastructure Operations (CAEIO). Reliable and secure IT systems are essential to achieving the CA's global mission in support of DOS, and CAEIO will be the vehicle through which O&M services to support this critical IT environment will be delivered.

C.2 SCOPE

The scope of this effort is to provide IT O&M services to plan, engineer, implement, enhance, maintain, and operate CA's enterprise IT infrastructure. This includes operational support for the HW/SW platforms on which CA IT systems reside and operate as well as providing operational

support for CA applications and databases. This TO will provide support to new applications modernized through the CA ConsularOne Program, as well as existing legacy systems, infrastructure, and applications prior to being modernized and eventually decommissioned. The contractor shall provide 24 hours per day, seven days per week, and 365 days per year (24x7x365) O&M support for the global CA IT environment.

The primary place of performance shall be the CA Headquarters location in the National Capital Region (NCR/ SA-17); located at 600 19th ST. NW, Washington, D.C as described in H.2.2. The contractor shall provide a site within 30 miles of the DOS CA/CST Headquarters (NCR/SA-17), commensurate with the contractors' proposed solution. The contractor's site shall meet all the requirements of Section H.4.2. The Government anticipates that the transition period for this task order will require the consolidation of five separate requirements into a single task order. Additionally, the requirements surrounding obtaining OpenNet connectivity approval for the contractor site is expected to occur during transition. Long-distance travel may be required to provide temporary support for global CA/CST sites.

The major task areas are identified below:

Task 1: Program Management
Task 2: Operations and Maintenance (O&M)
Task 3: Redundancy and Disaster Recovery (DR)
Task 4: Engineering and Implementation
Task 5: Acquisition and Asset Management

C.3 INFORMATION TECHNOLOGY (IT)/ NETWORK ENVIRONMENT

The global CA IT environment operates at multiple Consular facilities including overseas locations. This environment encompasses approximately 300 posts, two DOS domestic Data Centers, 29 Passport Agencies, two domestic Visa Processing Centers, and one non-production environment that is accessed from multiple locations and used for systems development and independent verification validation work. At each Consular facility, CA/CST supports the IT infrastructure in place to provide local processing for approximately 90 CA/CST applications, 1400 Oracle databases, and 500 Structured Query Language (SQL) databases.

At overseas posts, CA/CST/SO remotely supports the locally installed server backup and storage infrastructure, CA applications, and Oracle databases supporting consular functions at the respective post. At the domestic Visa Processing Centers; similar infrastructure, applications, and Oracle databases are in use. At the domestic Passport agencies; CST/SO supports the locally installed server and storage infrastructure, network devices that enable connection to the DOS network, CA applications, and Microsoft SQL databases that support passport processing capabilities. CA IT infrastructure installed within the domestic DOS Data Centers support centralized applications and replicated databases, along with central services and tools that support the CA IT environment.

The remote Consular locations connect through the Wide Area Network (WAN) to two domestic Data Centers where CA infrastructure supports centralized databases and applications. The Data Center infrastructure consists of converged server/storage solutions running Windows Server, Oracle Enterprise Linux (OEL), or RedHat Linux. Specialized equipment supports the Oracle databases, including Oracle Exadata storage devices and Zero Data Loss Recovery Appliances

(ZDLRAs) for redundancy and recoverability. Converged server/storage and disk backup solutions support the database and applications environment within the Data Centers.

CA/CST has a small cloud footprint today, but is developing a cloud strategy to guide cloud migration planning and it is expected that during the life of this TO, some portion of CA/CST supported services will migrate into a cloud environment. Today, Amazon Web Services (AWS) hosts static, CA travel information for access by the public. AWS is also used today to support load testing for a public facing CA applications. An IRM-managed Cloud Program Management Office (PMO) is guiding Department wide cloud initiatives, focused on moving email and other office automation services to the Microsoft O365 platform, SharePoint Online and Infrastructure as a Service (IaaS)/Platform as a Service (PaaS) solutions through Azure and AWS. Service Now will be used to host ITSM requirements for the Department. The contractor is responsible for supporting CA/CST in working with the IRM Cloud PMO on the ongoing O365, SharePoint Online and Service Now migrations. CA/CST is also working to determine how existing and planned Department-wide cloud solutions can be used to support CA requirements, and where there are gaps in capabilities. CA/CST is exploring other cloud offerings, for example Salesforce and Oracle Cloud.

C.3.1 ORGANIZATIONAL ENVIRONMENT

Within the DOS, there are several organizations with which CA/CST closely coordinates for planning, implementing, and supporting the IT Environment. The CAEIO contractor will have to collaborate/coordinate closely with these organizations in order to perform successfully on this contract. The information provided in this section is not all encompassing; the primary organizations are described below.

Some enterprise services are provided by a DOS entity outside of CA, the Office of Information Resources Management (IRM). IRM provides enterprise IT services including:

a. Facilities management of DOS Data Centers, including providing space, power, network connectivity, Heating Ventilation and Air Conditioning (HVAC), and general facilities management support.
b. Global network services, including providing network connectivity for CA domestic and overseas sites.
c. Network security services, including management of DOS firewalls, intrusion detection and prevention, and Information Assurance (IA) support for DOS.
d. Facilities management of Server Rooms at overseas posts in which CA/CST infrastructure supports CA applications and databases. Local IRM IT staff provide the "hands-on" support to enable remote administration, troubleshooting and problem resolution of CA assets by CA/CST technical teams.
e. End-user support, including desktop support, for CA users at overseas posts and some CA Headquarters users.

Effective communications and coordination with IRM technical teams is required.

Diplomatic Security (DS) is the Federal law enforcement and security bureau of the DOS, tasked with securing diplomacy and protecting the integrity of U.S. travel documents. DS mainly interacts with CA in the area of travel document fraud investigation as well as security. DS' network of investigators in the U.S. and around the world, investigates passport and visa fraud –

Federal felonies often committed in connection with other crimes, which is critical to securing U.S. borders and protecting U.S. national security.

In the area of Cybersecurity, DS safeguards the DOS' information and IT assets at more than 270 locations around the world. This includes protecting a global cyber infrastructure comprising of networks and mobile devices. DS provides Department-level network monitoring, cyber incident handling, cyber threat analysis, compliance verification and vulnerability analysis, cyber security policy and configuration development, cyber security awareness and training, as well as administration of the Regional Computer Security Officer (RCSO) program. CST, through its Information System Security Officer (ISSO), works with DS to perform Assessment and Authorization (A&A) requirements and to perform continuous monitoring, manage consular applications and servers, perform routine security audits for its servers, and regulate physical security.

Finally, DS conducts personnel security background investigations for the DOS and other Federal agencies.

The General Services Division (GSD) is a division under the Office of the Executive Director (EX) that coordinates/collaborates with CA's Asset Management team. This collaboration includes, but is not limited to the following:

a. Requesting bar codes from GSD for new equipment entering into service.
b. Providing the inventory list from GSD for the annual audit of all bar coded equipment in domestic locations that house CA equipment. The reconciling of that list during the annual audit is done in collaboration with GSD and CA's asset management.
c. Providing CA's asset management with Blackberries, iPhones, and iPads for CA customers requesting and approved for those items.
d. Coordinating with GSD for the installation of stand-up desks.

C.4 OBJECTIVE

The objective of the CAEIO effort is to deliver world class (O&M) support to the CA IT environment, provide outstanding customer service for the CA users, and implement proactive automated technical solutions to continuously improve the CA IT environment. Inherent to this task is collaborating within the integrated environment across the various task areas within this TO and with other stakeholders in the CA enterprise. The CAEIO contractor will recommend and guide the adoption of operational best practices and information sharing across the enterprise. This will enable CA/CST to foresee the needs of its internal IT customers, make informed enterprise IT decisions and investments, and rapidly respond to mission priorities. CA is adopting an Agile/Lean approach for project management across the applications/services development area and intends to extend the use of the Scaled Agile Framework (SAFe Agile) to all operations, maintenance, and engineering projects in the near term. A Development, Security, Operations (DevSecOps) (i.e. Continuous Integration/ Continuous Delivery (CI/CD)) methodology is being implemented to guide automated solutions for development, deployment, and operations within CST. The contractor shall adhere to the CA/CST project management practices and guidelines that facilitate this approach.

Through this TO, the contractor is responsible for providing services that meet these high level goals:

a. Reduce unplanned downtime for critical CA services through highly effective and proactive management of the IT environment.
b. Reduce impact to operations from failed deployments and changes to the IT environment through effective planning, testing and deployment of approved changes/fixes/updates to the existing environment.
c. Develop flexible and agile processes to perform preventative actions that lead to proactive detection of problematic incidents, issues and resources.
d. Propose and support automation of repetitive, impactful events/incidents and manual processes that improve standardization and lead to a reduction in errors.
e. Provide the ability and implement self-learning/self-healing or corrective actions to enhance the operational environment.
f. Provide development and ease of deployment, seamless integration, and real-time views into infrastructure that have multiple platforms, providers, and equipment.
g. Provide rapid response to alerts, incidents, and disruptive conditions.
h. Adapt to the current and future demands of the overall CA/CST mission and strategy.
i. Enhance and expand the Tier 0 capability to improve customer support across the enterprise.
j. Improve the quality of the operational status communications to the CA end users.

C.5 TASKS

C.5.1 TASK 1—PROGRAM MANAGEMENT

Strong Program Management is required across the broad scope of this Performance Work Statement (PWS). The contractor is responsible for effective management and administration of all efforts performed under this TO. The contractor shall provide program management support under this TO. This includes the management and oversight of all activities performed by contractor personnel, including subcontractors, to satisfy the requirements PWS.

The contractor shall designate a Program Manager (PgM) by name, for all programmatic issues, concerns, and status of the program. Under this task the contractor will be responsible for overall resource management; quality, risk, scope, schedule, communication management, and quality assurance. The contractor is responsible for scheduling meetings and providing deliverables in accordance with **Section F** of this TO.

C.5.1.1 SUBTASK 1 —COORDINATE A PROGRAM KICK-OFF MEETING

The contractor shall schedule, coordinate, and host a **Program Kick-Off Meeting (Section F, Deliverable 01),** at the location approved by the Government after Task Order Award (TOA). The meeting will provide an introduction between the contractor personnel and Government personnel who will be involved with the TO. The meeting will provide the opportunity to discuss technical, management, security issues, travel authorization, and reporting procedures. At a minimum, the attendees shall include Key contractor Personnel, representatives from the directorates, other relevant Government personnel, the CA/CST Government Technical Monitor (GTM), and the Federal Systems Integration and Management (FEDSIM) Contracting Officer's Representative (COR).

The contractor shall provide a **Program Kick-Off Meeting Agenda (Section F, Deliverable 02)** for review and approval by the FEDSIM COR and the CA/CST GTM prior to finalizing. The agenda shall include, at a minimum, the following topics/deliverables:

a. Points of Contact (POCs) for all parties.
b. Personnel discussion (i.e., roles and responsibilities and lines of communication between contractor and Government).
c. Staffing Plan and status.
d. Transition-In Plan and discussion.
e. Security discussion and requirements.
f. Quality Management Plan.
g. **Earned Value Management (EVM) Plan,** (**Section F, Deliverable 06**).

The Government will provide the contractor with the number of Government participants for the Kick-Off Meeting, and the contractor should provide sufficient copies of the presentation for all present. The contractor shall provide minutes of the **Program Kick-Off Meeting** (**Section F, Deliverable 03**).

The contractor shall schedule and coordinate a **Financial Kick-Off Meeting (Section F, Deliverable 04)** with the Government as a separate breakout session during the Program Kick Off Meeting. The meeting will provide an opportunity to discuss expectations for financial reporting, invoice requirements, and any other financial requirements of the TO.

C.5.1.2 SUBTASK 2—PREPARE AND PRESENT CONTRACT STATUS REPORTS (CSR)

The contractor is responsible for developing, submitting, and presenting a monthly **CSR (Section F, Deliverable 05)**. The contractor shall use the Government provided template (**Section J, Attachment E)**. The contractor is responsible for maintaining the CSR meeting minutes, and track and update CA/CST stakeholders, CA/CST GTM, and FEDSIM COR on all action items assigned during the monthly CSR meeting.

C.5.1.3 SUBTASK 3—EARNED VALUE MANAGEMENT (EVM)

The contractor is required to employ and report on EVM in the management of this TO**, (Section H.9).** The contractor will coordinate with the Government to determine which of the controls in the American National Standards Institute (ANSI) are applied to innovations and enhancements projects in order to ensure an optimal solution. The contractor is responsible for executing the EVM program controls for non-operational tasks where specified by the FEDSIM COR. EVM controls applied may vary from project to project as applicable. The contractor shall deliver an EVM plan in accordance with **section H.9** and **Section F, Deliverable 06**.

C.5.1.4 SUBTASK 4—WEEKLY ACTIVITY REPORTING (WAR)

The contractor Program Manager (PgM) shall prepare and submit two status reports -- the **Weekly Activity Report (WAR)** and the **Project Status Report (PSR) (Section F, Deliverable 07)**. The contractor will be responsible for conducting the WAR and PSR meetings with the CA/CST GTM, FEDSIM COR, and other Government stakeholders as required. The meeting for the WAR and PSR may be combined into a single meeting at the request of the Government. The contractor will maintain minutes of these meetings.

Briefing information for the WAR/PSR shall be prepared in accordance with **(Section J, Attachment F)**. The WAR is expected to include performance and relevant transition activities and ensure that the operational information from the prior week is summarized. The PSR is required to provide status of ongoing projects on a project by project basis to CA/CST and provide opportunities to identify other activities, establish priorities, and coordinate resolution of identified risks and issues.

C.5.1.5 SUBTASK 5—–PREPARE A PROGRAM MANAGEMENT PLAN (PMP)

The contractor is responsible for documenting all support requirements in a PMP. The contractor shall base the PMP on the CA/CST Service Strategy and Portfolio Management (SSPM) Program Control Process/ Requirements such as the System Development Life Cycle (SDLC) and SAFe Agile approaches to deployment with Project Management Guidelines. These requirements have been developed to aid CST management in oversight of all current and future programs/ projects that support CST's Enterprise Architecture. The contractor shall provide the Government with a **Draft Program Management Plan** (**Section F, Deliverable 08)** on which the Government will make comments. The **Final Program Management Plan (Section F, Deliverable 09)** shall incorporate the Government's comments.

The PMP shall:

a. Describe the contractor's proposed management approach and contain a detailed list of all Standard Operating Procedures (SOPs). (Note: The Government will provide the SOPs after award and the contractor is responsible for providing the detailed list of SOPs with the final PMP (Section F, Deliverable 09).)
b. Include milestones, tasks, and subtasks required in this TO.
c. Provide for an overall Work Breakdown Structure (WBS) with a minimum of three levels and associated responsibilities and partnerships between Government organizations.
d. Describe in detail the contractor's approach to risk management under this TO.
e. Include the contractor's communication plan describing in detail the contractor's approach to communications, including processes, procedures, communication approach, and other rules of engagement between the contractor and the Government.
f. Include the contractor's policy and procedures for telework.
g. Include the contractor's COOP plan for continuity of operational support for critical services provided through this TO in the event of a disaster at the contractors primary work location. Given space constraints within CA office space it is anticipated that the majority of contractor staff will work offsite at the contractor's site. In the event of a disaster at the contractor's site, the contractor will need to relocate staff to the government site or to telework locations to ensure continuity of support for critical services. The contractor shall document the proposed coverage approach in a COOP plan.

The PMP is an evolutionary document that shall be updated in accordance with **Section F, Deliverable 10.** The contractor shall work from the latest Government-approved version of the PMP. The contractor is responsible for ensuring the PMP is updated any time there is an adjustment to the program baseline.

C.5.1.6 SUBTASK 6—PROJECT SUPPORT

Project support allows for activity based managment for invidual activities such as POAM remediation, upgrades, support for ConsularOne applications, etc. The contractor is required to provide support for all projects executed under CAEIO. The contractor shall generate a **Project Plan**, as required (**Section F, Deliverable 11**) and any **Project Plan Updates** (**Section F, Deliverable 12**), on a project by project basis. Each project plan and schedule is required to be maintained and updated to reflect progress after each, status update, review, or milestone change. There will be approximately 50 projects per year. Project plans must include at a minimum:

a. Project charter
b. Project objectives
c. Project schedule
d. Project scope
e. Project tailoring
f. Work Breakdown Structure (WBS)
g. Level of Effort (LOE) estimate
h. Schedule (planed and actual dates).
i. Control gates
j. Milestones
k. Deliverables
l. Risk and issue register
m. Project staffing/resource loading
n. EVM (if applicable depending on dollar value of the project)

Project schedules for some projects may be integrated with CA/CST's Integrated Master Schedule (IMS) for review by CST Management. The contractor is expected to provide timely and accurate schedule updates as requested.

C.5.1.7 SUBTASK 7—PREPARE TRIP REPORTS

The Government will identify the need for a **Trip Report** when the request for travel is submitted in accordance with Section H.10.2 Travel Authorization Requests (TARs). The contractor shall deliver Trip Reports (**Section F, Deliverable 13**) with a summary of all long-distance travel including, but not limited to, the name of the employee, location of travel, duration of trip, and POC at the travel location. Trip Reports shall also contain Government approval authority, total cost of the trip, a detailed description of the purpose of the trip, and any knowledge gained. At a minimum, trip reports shall be prepared with the information provided in **Section J, Attachment J.**

C.5.1.8 SUBTASK 8—QUALITY MANAGEMENT PLAN (QMP)

The contractor is required to identify and implement its approach for providing and ensuring quality throughout its solution to meet the requirements of the TO. The contractor's Quality Management Plan (QMP) will describe the application of the appropriate methodology (i.e., quality control and/or quality assurance) for accomplishing TO performance expectations and objectives. The contractor's QMP is required to identify how it will manage and implement process improvements on a continuous basis in an effort to improve both the timeliness and quality of services and work products executed under this TO. The QMP must describe how the appropriate methodology integrates with the Government's requirements.

The contractor shall update the **QMP** and then provide a **final QMP** as required in Section F (**Section F, Deliverable 14**). The contractor shall **update the QMP**, as required in Section F **(Section F, Deliverable 15),** as changes in program processes are identified.

C.5.1.9 SUBTASK 9—TRANSITION-IN

The contractor shall provide a final **Transition-In Plan (Section F, Deliverable 16)** as required by **Section F**. The contractor is responsible for ensuring that there will be minimal service disruption to vital Government business and no service degradation during and after transition. The contractor shall implement its Transition-In Plan No Later Than (NLT) ten calendar days after award and ensure completion of transition activities within 120 calendar days from project start.

Contractor access to OpenNet is required for full functionality and successful performance on this TO. Contractor access to OpenNet will be limited until connectivity is established at the contractor's site as described in **Section H.4.2**. Additional information on work accessibility and network access during the Transition-In period is available in **Section H.4.3** of the TO.

The contractor shall be prepared to execute all relevant task areas by the end of the transition period.

C.5.1.10 SUBTASK 10—TRANSITION OUT

The contractor is responsible for providing Transition-Out support when required by the Government. The **Transition-Out Plan, (Section F, Deliverable 17)** shall facilitate the accomplishment of a seamless transition from the incumbent to an incoming contractor/Government personnel at the expiration of the TO. The Government will work with the contractor to finalize the Transition-Out Plan. At a minimum, this Plan shall be reviewed and updated on an annual basis. Additionally, the Transition-Out Plan shall be reviewed and updated quarterly during the final Option Period.

In the Transition-Out Plan, the contractor shall identify how it will coordinate with the incoming contractor and/or Government personnel to transfer any SW, HW, and other equipment/physical materials, as well as knowledge regarding the following:

a. Project management processes
b. POCs
c. Location of technical and project management documentation
d. Status of ongoing technical initiatives
e. Appropriate contractor–to–contractor coordination
f. Transition of Key Personnel
g. Schedules and milestones
h. Actions required of the Government

The contractor is responsible for establishing and maintaining effective communication with the incoming contractor/Government personnel for the period of the transition via weekly status meetings or as often as necessary to ensure a seamless transition-out.

The contractor shall implement its Transition-Out Plan NLT six months prior to expiration of the TO.

C.5.1.11 SUBTASK 11—INTEGRATED OPERATIONAL DASHBOARDS

The contractor is responsible for developing an integrated dashboard solution that will provide program based views, available to senior management and provide user based views for operational/technical staff. The integrated dashboard capability will have a dual purpose, to inform CA/CST management as well to provide technical staff with the appropriate monitoring and alerting solutions for operating and maintaining the enterprise IT environment. The integrated dashboard will be based on the capabilities developed and managed through the **Enterprise Monitoring** T**ask** (**C.5.2.9**).

The objective of the dashboards is to provide high level views to inform senior CA/CST management on the enterprise health of the environment by providing near-real time availability, capacity, security, and performance data with the ability to analyze trends and data metrics. Additionally, incident and ticket information shall be available in the management view to aid CA/CST senior staff in effectively managing problem resolution.

C.5.1.12 SUBTASK 12—PREPARE A QUARTERLY SPEND PLAN

The contractor shall submit and maintain a **Quarterly Spend Plan (Section F, Deliverable 18**) that reflects the projected spending for the upcoming 12 months. This must include a detailed break out of the following:

a. Task
b. CLIN
c. Contractor functional role
d. Employee status (exempt, non-exempt, subcontractor)
e. Employee name
f. Alliant 2 labor category
g. Subcontractor(s) company name(s), if applicable
h. Hours and dollars, per contractor functional role for each option period and month within the option period
i. Rate information (i.e, burden and unburdened) for each respective plan month
j. Totals of hours and costs by CLIN and Task Number
k. Non-labor costs
l. Grand total hours/costs by Task Number
m. ODCs
n. Tools

C.5.2 TASK 2–OPERATIONS AND MAINTENANCE (O&M)

The contractor shall provide O&M support for the CA IT enterprise including, but not limited to; Systems Administration (SA), database administration and support, infrastructure management, applications support, network administration, security operations, monitoring and proactive management of the CA IT environment, and customer support via the Service Center.

The contractor is required to support IT service operations 24x7x365 inclusive of Federal holidays and inclement weather closures for all tasks supporting the Operations and Maintenance (O&M). The contractor shall ensure all work being performed at a non-Government site that has approved OpenNet connectivity in accordance with **section H.4.2** of this TO.

The contractor shall provide Tier 0, Tier I, Tier II, and Tier III technical support for infrastructure, SQL databases, monitoring, and security operations for the CA environment. The contractor shall provide Tier 0, Tier I, and Tier II support for Oracle Databases and CA Applications, while other contractors outside of CAEIO will be responsible for Tier III support for these services.Tasks shall be managed at the Tier II level as they are transitioned from Tier III support teams external to CAEIO. The contractor is responsible for collaboration across task areas to ensure the IT environment remains highly available.

The following tier descriptions indicate the levels of support necessary to resolve incidents across the enterprise:

a. Tier 0: is support available to customers that does not require directly interacting with a customer advocate.
b. Tier I: is defined as providing initial support for basic client needs. The contractor at this level is responsible for gathering customer information and making a determination of the customer issue by analyzing the symptom(s) and the underlying problem(s). Once the problem(s) has been accurately identified and logged into the Ticket Management System, the contractor tries to resolve the client's problem(s). Problems not resolved at this level shall be escalated to Tier II support. Tier I retains Total Ticket Ownership of the incident/problem(s).
c. Tier II: is defined as providing a higher level of support than Tier I with greater technical expertise and more in-depth knowledge about a particular product or service. Tier II support performs routine maintenance across the environment and are responsible for monitoring and proactive management of the CA IT environment. Tier II support assists the Tier I personnel in solving technical problems or investigating elevated issues by confirming the validity of the problems and seeking known solutions to more complex problems or issues. If a problem is new and/or cannot resolve it at this level, it shall be elevated to Tier III technical support. Certain repeatable tasks which historically may have been performed by the Tier III support teams (i.e. other contractors) may be transitioned, upon Government approval, to CAEIO.
d. Tier III: is defined as providing the highest level of technical support. This level of support handles the most difficult and advanced problems. Tier III support performs expert level troubleshooting and analysis of issues and problems. Tier III support assist Tier I and Tier II with research and development of solutions to new or unresolved issues. When a solution to the problem is determined, Tier III support is responsible for designing and developing one or more courses of action, evaluating each of these courses in a test case environment, and implementing the best solution to the problem(s). The contractor shall verify the solution and ensure successful delivery to the client. The problem or issue now becomes a known issue or problem and can be addressed at Tier I or Tier II support.
e. Tier IV: is defined as requiring outside vendor or third—party support. The contractor is responsible for contacting and coordinating the repair/incident correction with the appropriate outside vendor.

In performance of the O&M Tasks, the contractor shall comply with all relevant DOS regulations, policies, acts/mandates, and standard procedures. The contractor shall be certified in International Organization of Standardization (ISO) /International Electrotechnical Commission (IEC) 20000 and CMMI-DEV Level III. The contractor shall utilize scalable processes and

techniques that allow for surges in activities, varying product priorities, and provide a standards based best practices approach to providing services. The contractor is required to follow CA/CST frameworks such as Waterfall SDLC, SAFe Agile, DOS Managing State Projects Methodology, and Project Management Institutes (PMI) Guide to Project Management Body of Knowledge (PMBOK) in the performance of this TO. The contractor shall follow Information Technology Infrastructure Library (ITIL) v3 and v4 (as applicable), National Institute of Standards and Technology (SP 800-53, 800-171), ISO/IEC 20000, 27002 Information Security, Quality Assurance Methodologies, and Enterprise Change Management Processes. The contractor shall comply with all regulations, policies, standards, certifications, and procedures; mentioned in the above paragraph, for all task areas in the performance of this TO.

C.5.2.1 SUBTASK 1–KNOWLEDGE MANAGEMENT (KM)

KM is essential to identification, maintenance, and management of data, information, and knowledge utilized in support of services provided by the contractor in preparation and support of CA/CST IT service offerings. The contractor shall develop a **Knowledge Management Plan (KMP)** (**Section F, Deliverable 19)**. The KMP will encompass all task areas of this TO. The KMP contains the contractor's approach to updating and maintaining the various documents housed in the KM database and SOPs. The contractor is responsible for maintaining and enhancing existing SOPs, and developing and maintaining new SOPs to ensure consistent support of the environment. The contractor is responsible for maintaining and enhancing existing Knowledge Based Articles (KBAs); and developing and maintaining new KBAs as required for use by CA/CST IT teams, as well as, by CA users to ensure that standard approaches are used to resolve common problems. The contractor is required to coordinate at least semi-annually, or as required, across the enterprise to obtain updates from the responsible stakeholders for the SOPs and KBAs. KM documentation may include, but is not limited to the following items:

a. Systems Documentation: information about the systems, applications, databases, and services installed and/or configured. (This information may be used and or developed for maintenance across all support tiers).
b. "As is" IT infrastructure diagrams: logical and physical diagrams that depict the CA IT environment with systems and data flows.
c. Information security policies, procedures, and documentation.
d. Technical requirements.

The contractor shall maintain and optimize existing KM repositories and databases to allow for maximum efficiency; and may utilize existing tools, to support CA/CST and inform the enterprise and its stakeholders. Existing tools to support KM include but are not limited to Remedy, SharePoint, Jira, Confluence, Rational tools (Collaborative Lifecycle Management (CLM) tool, Clear Case, and Clear Quest), Visual Source Safe (VSS), and Shared Drives. KM will enable collaboration, content management, records management, and business process management. The contractor is responsible for providing standardized structures (taxonomies) for tagging content. The contractor is responsible for providing appropriate individual, Role-Based Access Control (RBAC). The contractor is required to store and organize content in a way that it can be efficiently searched.

The contractor is required to provide KM support services that streamline and improve KM processes such as self-help initiatives. The contractor shall facilitate, train, and sustain the ability of KM users to interface with IT operations. The contractor is responsible for

improving KM integration with the IMS, SharePoint, Integrated Operational Dashboard, and other monitoring tools to ensure maximum user access to a self-service KM environment based upon authentication and authorized use.

The contractor shall also provide documentation and technical writing services that are typical of IT projects and in support of CA/CST initiatives; these tasks must include, but are not limited to:

a. Developing and maintaining documentation related to the ITIL processes and/or on-line sources of data.
b. Developing and maintaining training materials and documentation.
c. Developing and maintaining systems documentation, including logical and physical diagrams of the IT infrastructure supporting each system.
d. Providing analysis based on KM tools to serve as input for changes in SOPs.
e. Developing and maintaining SOPs to include the Tactics, Techniques, and Procedures (TTPs) for each support role in this TO (i.e., web administration, desktop support, and active directory administration).
f. Maintain a centralized knowledge-base/repository (i.e. KBAs and SOPs). Manage the process, content, visibility, retrieval methods and ensuring the search capability is user friendly and available at all times.
g. Conduct semi-annual and as needed re-reviews of KBAs; request semi-annual reviews and as needed provide support for other groups to re-review KBAs.
h. Develop and maintain websites that support CA/CST operational support documentation and services. Currently the websites are maintained in SharePoint, Adobe Experience Manager, and Confluence.

C.5.2.2 SUBTASK 2—PROVIDE SERVICE CATALOG/PORTFOLIO MANAGEMENT

The contractor shall assist CA/CST in managing an enterprise level IT service portfolio/catalog that provides customers with a pre-defined set of available products and services for the various task areas covered by this TO (Service Center, Infrastructure Support, Database Support, Application Support, Enterprise Operations Center, Network Operations, Configuration/Change Management, Capacity and Performance, Security Operations, and Engineering/Implementation). The contractor is responsible for identifying, prioritizing, and recommending additional service opportunities that create business value. The contractor shall manage the portfolio/catalog of services delivered under this TO. The contractor is required to maintain a complete and accurate service pipeline of all services under development; a catalog of all operational services, and services available for deployment; and a repository containing information about services that are phased out or retired.

C.5.2.3 SUBTASK 3—INFRASTRUCTURE ARCHITECTURE AND STANDARDS SUPPORT

CA/CST is responsible for establishing the IT enterprise architecture for CA systems and services; and for ensuring new and/or updated systems, services, and infrastructure are designed to comply with the enterprise architecture. CA/CST Government teams manage and lead governance processes intended to monitor compliance. The contractor shall provide technical expertise, develop documentation for review by the boards, and support coordination through the process. These governance bodies include:

a. Investment Review Board (IRB)—The IRB is comprised of senior CA/CST managers and tasked with reviewing CA IT initiatives to determine appropriate business justification and alignment with CA strategic goals. Additionally, the IRB determines whether competing or similar initiatives are already in process to prevent redundancy and duplicative spending, and whether the new project affects the resources or timelines for existing projects.
b. Architecture Review Board (ARB)—The ARB is responsible for establishing and maintaining Enterprise Architecture standards to which all CA/CST initiatives must comply. The ARB advises the IRB on issues and opportunities that pertain to the successful investment in, and delivery of, infrastructure and solution architectures to internal and external consumers of CA/CST IT services. The scope of the ARB authority includes, but is not limited to review and approval of technology choices and implementation approaches proposed by all divisions within CA/CST.
c. CA Configuration Control Board (CCB)—The CCB reviews and approves all proposed new/ upgraded SW and HW components to establish the CA baseline.
d. CA Enterprise Change Board (ECB)—The ECB reviews and approves all proposed changes to the CA IT operational environment.
e. Firewall Advisory Board (FAB) - The Firewall Advisory Board (FAB) reviews, approves, and tracks configuration changes to the Department-level firewalls. IRM is the chair of the FAB. The responsibilities of the board include the following:
    1. Establishing baseline configurations for all Department-level firewall installations;
    2. Establishing criteria to control connectivity of non-Department of State organizations to Department networks;
    3. Receiving all requests for changes to the Firewall Rule Set, performing a risk assessment of each request, and authorizing appropriate changes to the rule set;
    4. Recommending changes to the firewalls and network architecture to improve network security;
    5. Providing assistance in developing firewall-related solutions to meet the operational requirements of new network applications; and
    6. Reviewing the Firewall Rule Set annually

In addition to the above governance boards, CA/CST projects are managed using the SDLC with stage gate reviews managed by CA/CST Government staff that review and approve all projects to move forward to deployment. The SDLC process governs traditional waterfall efforts and is being phased out as SAFe Agile becomes the standard for CA/CST project management.

C.5.2.3.1 INFRASTRUCTURE ARCHITECTURE DEVELOPMENT SUPPORT

The contractor is responsible for proactively contributing to the development and maintenance of infrastructure architectures for the CA IT environment. The contractor is responsible for the translation and estimation of architectural directions into support requirements, including impact on current support operations and capabilities, risk analysis of proposed migrations, and supportability of new technologies. The contractor shall assist CA/CST with strategy formulation through discussions with technology subject matter experts and conducting research related to infrastructure architecture.

C.5.2.3.2 INFRASTRUCTURE STANDARDS SUPPORT

The contractor shall assist CA/CST with IT infrastructure standards development, in moving toward standard configurations across the entire organization, and documenting and maintaining infrastructure standards. In addition, the contractor is responsible for assisting the ARB in communicating infrastructure standards, and assisting in the governance efforts, including but not limited to those conducted by the boards defined in this section, to include IRB, ARB, CCB, and ECB. The contractor is responsible for researching, designing, and recommending processes to achieve standardization of the services, and technical solutions based on business needs, third-party contractor products and services, and infrastructure requirements.

C.5.2.3.3 LONG RANGE SYSTEM PLANNING

The contractor is responsible for evaluating and recommending appropriate tools and processes that enhance the stability and functionality of the environment, and allow provision of services in accordance with CA/CST's Enterprise Architecture and infrastructure standards. The contractor shall assist CA/CST with long-range system plans by providing the following services, at minimum, but not limited to:

a. Compare and assess requirements against the current installed infrastructure architecture, as well as, the future planned infrastructure architecture to assess the impact.
b. Support CA/CST permanent and ad-hoc committees and working groups addressing such issues.
c. Identify opportunities to consolidate devices and services, utilize new technologies, and improve the delivery of services.

C.5.2.4 SUBTASK 4—SERVICE CENTER

The primary function of the Service Center is to oversee the provision of end user services, including, but not limited to the following: incident management and tracking; processing of IT service requests; ticket escalation for service events; operational communications and notifications; initial triaging and troubleshooting of service events within the CA IT environment; CA application and service updates; limited mobile device support; desktop support; problem management; contributing to, creating, and managing KBAs and SOPs; and confirming SW licensing and available inventory to fulfill service requests.

C.5.2.4.1 SERVICE DESK (SD)

The SD directly supports CA's Service Center and is the first and central POC for customer service for all service events related to the CA IT infrastructure environment. As such, providing superior and professional customer service and Tier I support to the CA/CST internal user community is an important function of this task. Service events are defined as: incidents, problems, service requests, or change requests made through a variety of communication methods (i.e. email, phone, instant message, walk-in, notification using the Ticket Management System, or automatic report of an event).

The contractor shall provide responsive SD support to all users. The contractor is responsible for receiving the initial contact requiring technical support, opening and tracking the service event

within the Ticket Management System, and monitoring all to resolution as described in the **Total Ticket Ownership (TTO) Section C.5.2.4.2** of the TO.

The SD is responsible for coordinating, troubleshooting, diagnosing, and resolving all incidents and problems through to closure. This will require collaboration across CA/CST technical support teams, including teams not managed through this TO, and may involve external technical teams in troubleshooting. The contractor shall ensure that a callback and line queuing service is offered to resolve high call volume scenarios. The contractor must ensure that voice/digital communications are managed effectively across all support groups and information is channeled and escalated between teams based on the incident or service request priority.

The contractor shall prepare and distribute a Daily Operations Report and conduct Daily Status Reviews (DSRs) with Government stakeholders; which convey the operational status of the CA IT environment and the status of the enterprise operations for incidents, problems, changes requests, both successful and rollbacks; outages (planned /unplanned).

The contractor shall provide, develop, install, implement, administer, and maintain an Automatic Call Distribution (ACD) telemetry system. The ACD system shall support answering and managing phone calls for service request resolution. The ACD is required to provide a scalable solution including a call menu with the capability to facilitate a real-time call log, call monitoring, accounting, and reporting for efficiency of call handling.

Tier I support shall be performed primarily at the contractor's site. The Government may move Tier I support to the NCR Headquarters location during the period of performance of the TO; however, there is not a time frame currently available for this move.

The contractor is responsible for providing support to infrastructure that enables successful data, voice, and video communication at its offsite location, required to successfully perform the tasks outlined in this TO. The contractor is responsible for coordinating with internal and external providers/carriers during service events; this includes providing cleared facility escorts for outside service providers.

C.5.2.4.2 TOTAL TICKET OWNERSHIP (TTO)

IT Service Management (ITSM) is required across several tasks, and is not limited to the SD. However, the SD is required to coordinate Incident/Service Request Management across CA/CST. The contractor is responsible for performing and providing root cause analysis for all tickets, for which full management is within CAEIO. The contractor is responsible for coordinating root cause analysis efforts across CA/CST technical teams for incidents and/or problem tickets.

The contractor shall adhere to CA/CST policies and procedures for service events/tickets, logging, documentation, and prioritization. The contractor shall utilize a Ticket Management System. Currently, Remedy is the system used for ticket management; however, this may evolve or change during the period of performance for this TO. The Government will provide the capability for CA/CST-identified monitoring and alerting systems to automatically access the CA ticketing system. The contractor is responsible for supporting, planning, and managing escalation and transition between the various tiers of support required.

The contractor is responsible for developing, coordinating, administering, updating, and submitting change requests to maintain all required workflows in the Ticket Management

System. The contractor is responsible for assisting with recommendations for systems enhancements for all hardware, software, process, and procedures used to support the Service Center's offerings. The contractor shall provide the following services, but not limited to:

a. Ticket Management System: The contractor shall communicate, coordinate, collaborate, review and validate changes to the Ticket Management System configuration and organization to maintain and enhance the functionality of its services and capabilities. Based on the elevated access the contractor has to the Ticket Management System, the contractor shall update information as necessary to user accounts and other information.
b. Incident Classification Process: The contractor shall review, recommend, and revise as necessary a Configuration Management Set of Classifications to be used in categorizing incidents logged into the ticket management system. The contractor is responsible for recommending and coordinating updates to the services as necessary to accommodate the defined classifications. The Government will participate in the creation of the classifications.
c. Incident Prioritization: The contractor shall assign priorities to tickets based on the level of priority and need for resolution in accordance with the Priority Escalation and Criticality Table. Provide Daily Status Review (DSR) report and meeting support for priority 1 and 2 tickets as required.
d. Resolution Classification Process: The contractor is required to develop an Incident Resolution Set of Classifications to be used in categorizing the root cause of incidents. The contractor shall update the Ticket Management System as necessary to accommodate the defined resolution classifications. The Government will participate in the creation of the classifications.
e. Self-Help and Service Requests: The contractor is responsible for enhancing and maintaining the self-help/self-service request capability. This includes, but is not limited to, allowing users to search and find information, advice, or standard processes they can use to resolve their own issues and fulfill standard requests such as password changes or software requests. Service requests shall include, but are not limited to, HW/SW requests, licenses, account provisioning, and account management.
f. Problem Management: The contractor shall coordinate root cause analysis efforts across CA/CST technical teams for high or critical incidents, or recurring medium priority incidents, for which no clear cause has been determined during initial troubleshooting. The contractor shall create a Problem Management Investigation (PBI) ticket and track it to resolution. The contractor is required to perform trend analysis for reoccurring system events, service interruptions, outages etc.… in order to manage potential problems proactively as well as reactively.

C.5.2.4.3 NOTIFICATIONS

The SD is responsible for enhancing and maintaining the notification procedures and SOPs to provide status on all service incidents. The contractor shall provide a **Notification Plan** (**Section F, Deliverable 20**) to include directives and guidelines for all CA/CST and non-CA/CST notifications and advisories that apply to scheduled and unscheduled outages, release management, and SW or HW deployments. The contractor is responsible for creating and issuing operational notices to update CA customers and CA/CST management of critical incidents.

C.5.2.4.4 DESKTOP SUPPORT

The contractor shall provide technical support of desktop, applications, and related technologies for all CA/CST users in accordance with DOS policies and procedures, ensure all desktops meet minimum requirements, and provide proactive and reactive surge desktop support Tier II services. The contractor shall ensure that all problems/incidents are logged into the Ticket Management System and managed in accordance with the **TTO Section (C.5.2.4.2)** of the TO. This desktop support includes, but is not limited to:

a. Provide a migration strategy and project plan for new/additional automated tools as required, if requested by the FEDSIM COR and/or CA/CST GTM.
b. Install, configure, troubleshoot, resolve complex issues, and support ongoing usability of desktop computers, laptops, SW/HW, and peripheral Commercial-Off-the Shelf (COTS)/ Government-off-the-Shelf (GOTs) technology.
c. Assess desktop functional needs to determine specifications for purchases on all break/fix/ move related issues or requests as well as targeted desktop expansions of approximately 20 desktops or less in the facilities noted in **Section J, Attachment K**.
d. Ensure all desktops/laptops meet approved and required patches.
e. Install and Troubleshoot DOS approved Government Furnished Equipment (GFE) for break/fix /move related issues or requests, as well as targeted desktop expansions of approximately 20 desktops or less in the facilities noted in **Section J, Attachment K**.
f. Install and troubleshoot DOS approved and issued laptops, iPads, Blackberries, and other mobile devices, as required by the FEDSIM COR and/or CA/CST GTM.
g. Maintain and support crisis management kit to ensure compliance with all current patches and updates. The kit inventory includes, but is not limited to, laptops, routers, and switches.

C.5.2.5 SUBTASK 5—INFRASTRUCTURE MANAGEMENT

The contractor shall manage, operate and maintain core infrastructure services across the CA IT enterprise in support of DOS strategic goals. Services shall include Data Center Management, Infrastructure Support, Card Printer Support for Domestic Locations, Domestic Consular Office Systems Administration (SA), Web Services Administration-Infrastructure, and Enterprise IT Service Operations.

C.5.2.5.1 DATA CENTER MANAGEMENT

The contractor shall provide data center management services to support CA IT infrastructure installed within the DOS data centers. The contractor shall ensure that all problems/incidents are logged into the Ticket Management System and managed in accordance with the **TTO Section (C.5.2.4.2)** of the TO. This activity requires coordination with IRM, as the facility managers for all DOS data centers. The contractor shall:

a. Coordinate with other DOS entities (IRM) to:
    1. Oversee operations of the CA Data Centers' infrastructure.
    2. Minimize impact to CA operations during planned Data Center maintenance.
    3. Plan for buildout of new CA infrastructure for the Data Center, to include space, power, network and storage.
b. Coordinate delivery and implementation of CA equipment.
c. Manage the CA Data Center Access Control List and access to the Data Center.

d. Coordinate, review and manage POC information with IRM for all Enterprise Server Operations Center (ESOC) Outage notifications.

C.5.2.5.2 INFRASTRUCTURE SUPPORT

The contractor shall provide infrastructure support for CA servers, storage platforms, systems, networking equipment, and hosted systems in use at DOS facilities domestically and overseas. The contractor shall ensure that all problems/incidents are logged into the Ticket Management System and managed in accordance with the **TTO Section (C.5.2.4.2)** of the TO.

The contractor support shall include, but is not limited to:

a. Provide comprehensive technical support of all Consular infrastructure in use at DOS facilities.
b. Coordinate overseas assistance requiring local hands on support, with IRM as IRM staff provide local IT support for all overseas posts.
c. Provide Windows and Linux-based Server Hosting support, including but not limited to installing, managing, and maintaining Window/Linux DOS complaint server environments. This includes:
    1. Midrange server platform HW running enterprise mission applications and services (application, database, middleware, web portal, and / or proxy servers).
    2. VMWare virtualization clusters hosting of Windows and Linux servers on both internal (OpenNet) and multiple DOS Demilitarized Zones (DMZs) networks.
d. Perform system health checks and conduct proactive monitoring and performance management of servers including but not limited to analysis of Central Processing Unit (CPU) utilization, memory utilization, Input/Output (I/O), storage utilization and network interfaces.
e. Analyze and identify applications and services that degrade server performance.
f. Monitor and respond to alerts generated by the Enterprise Event Management and Monitoring capability.
g. Provide Preventative Maintenance (PM) and Remedial Maintenance (RM) for infrastructure.
h. Perform backups and restores of data.
i. Provide SW support, including but not limited to; operating systems, virtualization, SW authentications, SW utilities, and schedulers.
j. Support storage solutions globally including but not limited to, enterprise block, object and network attached storage, and managing multiple Storage Area Networks (SANs) housing multiple petabytes of data.
k. Support and resolve GOTS problems conferring with other DOS Bureaus that deploy and provide GOTS applications as needed.
l. Provide support for Oracle appliances (i.e. Exadata, Zero Data Loss Recovery Appliance (ZDLRA)) installed within the Data Centers to support the CA database environment.
m. Support and maintain security, backup, and load balancing appliances in the physical and virtual environments and direct support of databases and Enterprise Service Bus (ESB) (i.e. Layer 7, F5, and Avamor).
n. In conjunction with engineering and implementation, as well as other CA/CST teams; including engineering and deployment, plan and implement infrastructure refreshes.

o. Support the Business Intelligence Data Smart Infrastructure that currently supports enterprise reporting for CA.
p. Support authorized and vendor recognized patching for infrastructure.
q. Support, plan, and schedule remote or local backup/restore/recovery services.
r. Provide maintenance and monitoring support of the ESB environment and service with the latest version of services, patches and configuration in accordance with the engineering team's guidance and contractor recommendations.
s. Provide support for industry standard protocols (i.e. Windows Management Instrumentation/ Simple Mail Transfer Protocol (WMI and SMTP)).
t. Provide support for infrastructure audits, assessments, and compliance analysis.
u. Submit system baseline requests to meet DOS and CA/CST requirements prior to deploying new HW/SW.

C.5.2.5.2.1 CARD PRINTER SUPPORT FOR DOMESTIC LOCATIONS

The contractor is responsible for providing regularly scheduled on-site PM and on-call remedial repair of critical agency HW nationwide, including all contractor sites, to ensure that passport production services are uninterrupted. The card printers are currently located at 18 passport sites and two development and test sites in the DC Metro area (reference **Section J, Attachment K. T**wo models of card printers are currently in use, to include low and high volume printers. High volume card printers are installed in limited locations today including at both agency print centers Arkansas Passport Center (APC) and Tucson Passport Center (TPC) and test and development centers at two separate locations within the DC Metro area. The contractor shall ensure that all problems/incidents are logged into the Ticket Management System and managed in accordance with the **TTO Section (C.5.2.4.2)** of the TO.

The contractor is required to submit regular reports on its maintenance and repair activities to the FEDSIM COR and GTM. These reports will include performance, cost, schedule, and outcome statistics that demonstrate a real-time picture of the contractor performance.

The contractor shall provide PM and RM for passport card printers. PM refers to the scheduled procedures performed on a routine or recurring basis that keep the equipment in optimal operating condition throughout its serviceable life. RM is defined as unscheduled work repairs and services. PM includes the scheduled cleaning, lubrication, and systematic inspection of the equipment and the detection and correction of faults. PM and RM, including onsite development and test, will be performed on-site at CA locations.

The contractor shall provide a combined Preventative/Remedial Maintenance Plan (Card Printers) **(Section F, Deliverable 21)** in accordance with **Section F** that includes the frequency, duration, and quality of scheduled service, and necessary equipment for the maintenance of the card printers.

The Government will provide a work area for PM and repair at each site. The contractor is responsible for ensuring that maintenance and repair services for all HW equipment is available during all hours of agency/center operations, regardless of time zone. During possible peak season multiple shift operations, maintenance and repair services may also be needed outside of regular business hours, **(Section J, Attachment K)**.

The contractor is required to document all PM/RM performed on each printer. All maintenance records are the property of the Government and shall be accessible at all times to authorized

Government personnel. Upon expiration of the contract, all maintenance records will be transferred to the Government. These records should include performance, cost, schedule, and outcome statistics.

The contractor support includes, but is not limited to:

a. Provide the full array of PM/RM services on all card printers, including providing supplies. PM shall include all periodic cleaning, maintenance, replacement parts, refurbishment, calibration, and/or other adjustments of the card printers and related equipment as necessary. All PM/RM will be performed in accordance with the manufacturer specifications, manuals and other instructions. The contractor is responsible for ensuring that printers are operational during normal business hours. No printer will be without the capability to personalize passport cards for more than 24 hours.
b. Respond to customer requests for RM. Within four hours of receipt of service request, the contractor shall document and implement a mitigation strategy to remedy the issue.
c. Provide all supplies and consumable materials for the on-going operation of the card printers. Examples of consumables are ink, lubricants, aerosols, cleaning wipes, calibration cards for the vision system, isopropyl alcohol, greases, anaerobic sealant, Liquid Crystal Display (LCD)/plasma screen cleaners, Glue, glass cleaner, all-purpose cleaner. The contractor will not be required to provide card stock under this TO.
d. Maintain an inventory of all spare parts, supplies, and/or consumable in support of all card printers.
e. Ensure SW packages are maintained and current, including providing the latest SW updates, upgrades, and security patches.
f. Provide replacement parts/components as required to complete repairs. The contractor will be reimbursed for the cost of required replacement parts/components. Any card printer replacement parts that are not purchased from the OEM must be approved in writing by the CA/CST GTM and FEDSIM COR.
    1. The most commonly needed spare parts (in accordance with the Ticket Management System) are to be kept in inventory to support the high-volume printers. In the event a part is not in inventory at the APC/TPC, the part is overnighted to APC/TPC (a historical list will be provided at TOA).

C.5.2.5.2.2 DOMESTIC CONSULAR OFFICE SYSTEMS ADMINISTRATION (SA)

The contractor is responsible for providing all Domestic Consular facilities with the same level of technical support as referenced under the Infrastructure Management Section of the TO with the additional capability of supporting the nuanced HW/SW located at the Domestic Consular/Passport facilities.

The contractor shall provide SA support at all domestic Consular facilities, including Puerto Rico and Hawaii as defined in **Section J, Attachment K**. The contractor is required to provide SA support to augment Government SAs as requested. The contractor is responsible for reporting and centrally managing the activities of all SA's across the Domestic Consular Facilities. The SAs shall support the ISSO and ensure that security and internal controls are handled in accordance with DOS policies and procedures. The contractor SAs shall ensure that all problems/incidents are logged into the Ticket Management System and managed in accordance with the **TTO Section (C.5.2.4.2)** of the TO.

Contractor duties and responsibilities consist of the following IT related functions, including but not limited to:

a. Provide planning, installation, training, support, monitoring and maintenance of HW (server and workstation builds) and software including all CA applications (e.g., Active Directory accounts and passwords, System Center Configuration Manager (SCCM)/Post Administration Tool (PAT) (patching) tool, Travel Document Issuance System (TDIS), Passport Records Imaging System (PRISM), Automated Cash Register System (ACRS), and other locally installed CA applications, etc.) security/vendor patches/updates/vShepere Installation Bundle (VIBs), and Oracle/SQL databases.
b. The SAs should provide reporting of these efforts such as, but not limited to: Server/workstations rebuilds VMware and standalone environments (Windows and Linux), management of Windows, VMware, NetApp Filers, and Tape Libraries.
c. Coordinate and inform CA/CST management of all risks impacting IT related services including but not limited to, power outages, environmental changes, natural disasters (fire/flood), employee accident or deliberate acts, maintenance or third party vendor actions.
d. Coordinate and plan for upgrades, perform monthly restores to validate user data integrity, replace HW/SW components as needed, and prepare for consolidation and decommission/retiring of HW/SW.
e. Perform back-ups, restores, purges and on-going management of data, systems, software and HW.
f. Monitor and document abnormal performance of server, workstation, and services trends as well as document and maintain site topology configuration and changes.
g. Provide server/workstation security services.
h. Provide remediation of vulnerabilities and ensure Symantec Endpoint Protection (SEP) compliance on all required devices.
i. Provide all hardware and software maintenance, such as defective tape drives, tapes, hard drives, servers, workstations, chip/read writers, driver license readers, barcode readers, printers, digital scanners, etc.
j. Provide all Active Directory service/user account and password administration, and Active Directory user privilege administration and badge logon administration.
k. Create, maintain, track and communicate configurations and/or changes of configurations in HW, SW, data, permissions (or security-related information), etc.
l. Develop, maintain, and communicate diagrams, system configurations and technical documentation.
m. Provide and ensure availability, efficiency and effectiveness of systems, SW, HW, and data as well as technical support for testing and evaluation purposes.
n. Document, track and report on the support provided to the Consular facilities (inclusive of all levels of support and all Consular facilities); report and follow-up on all trouble calls.

C.5.2.5.2.3 WEB SERVICES ADMINISTRATION--INFRASTRUCTURE

The contractor shall administer and maintain the Apache web services hosted at all overseas locations. The Apache web services are used to host Consular applications and reports. Currently the Government uses PowerShell as the system to support web service automation, maintenance, monitoring, and development tasks.

C.5.2.5.3 ENTERPRISE IT SERVICE OPERATIONS

The contractor shall ensure that all problems/incidents are logged into the Ticket Management System and managed in accordance with the **TTO Section (C.5.2.4.2)** of the TO. The contractor shall operate and maintain services used across the CA IT enterprise including, but not limited to the following:

a. Active Directory (AD): Monitor CA's AD domain to provide authentication and authorization services for CA's organizational units in the NCR and domestic facilities. The contractor shall support CA/CST in liaising between CA and IRM for all AD requests and issues.
b. Exchange: Microsoft Exchange clusters (2010 or later) in data center facilities and Exchange servers (2010 or later) at CONUS facilities. (OCONUS facilities are the responsibility of a different contractor).
c. Domain Name System (DNS): Coordinate and collaborate, via CA/CST, with IRM to ensure all DNS implementation approaches conform to and integrate with DOS requirements and infrastructure.
d. Dynamic Host Configuration Protocol (DHCP): Manage DHCP scopes and leases for CA.
e. System Center Configuration Manager (SCCM): SCCM instances and patching of infrastructure. Operate over 45 SCCM servers on all enclaves that update and secure over 10,000 Windows servers and workstation clients. The contractor shall provide antivirus support and guidance for CA systems. The contractor shall provide server and application remediation for compliance, vulnerability, anti-virus, and patching.

C.5.2.6 SUBTASK 6 –DATABASE SUPPORT

The contractor shall provide database management support for identified CA databases to include Oracle (Version 11g or higher) and Microsoft SQL Server (Version 2008 or higher) platforms.

The contractor shall perform Tier II support for all databases and through Tier III for all SQL databases used by legacy and modernized, client/server and web-based applications. The contractor shall support modernized databases and assist in the transition towards modernization initiatives. The contractor is responsible for reducing operational downtime for critical, scheduled, and unscheduled maintenance by accelerating deployments of approved changes/fixes/updates and solutions and automate manual maintenance, deployment, diagnostic health checks, validation, and reporting. The contractor is responsible for performing proactive and reactive monitoring and responding to incidents, alerts generated via database monitoring SW implemented within the Enterprise Event Management and Monitoring capability. The contractor shall ensure that all problems/incidents are logged into the Ticket Management System and managed in accordance with the **TTO Section (C.5.2.4.2)** of the TO.

In addition, the contractor will provide the following support for all databases (including both Oracle and SQL) including, but not limited to:

a. Perform Tier II O&M on Consular Consolidated Database (CCD), associated databases, and other Oracle databases.
b. Perform O&M (through Tier III for SQL Databases).

c. Maintain CCD Based Web Services (CCDWS) used for data exchange/transfer, and Post CCD Web services.
d. Tune databases as required for optimal operational performance and generate performance reports to include usage optimization.
e. Deploy and maintain data interfaces into CCD and applications.
f. Support data storage HW/SW for identified production databases (e.g. Oracle Automatic Storage Management, Oracle Exadata, EMC Data Domain, and NetApp SANs).
g. Manage database resources across all platforms.
h. Perform backups (onsite and offsite/remote) and restores.
i. Maintain and support the Business Intelligence Data Smart Infrastructure including the following:
    1. Maintain and support heterogeneous environments in central, domestic, and overseas sites including physical, virtual, and cloud. (Cloud environments exist in a limited capacity; however, the intent is to migrate to cloud capabilities during the period of performance of this TO).
    2. Maintain capabilities for physical and virtual infrastructure management following Government guidance and protocols for emergencies.
j. Maintain and apply DOS authorized and vendor recommended patches.
k. Coordinate and support production troubleshooting as required.
l. Maintain and support the ESB including but not limited to:
    1. Maintain and support the Service Oriented Architecture (SOA) ESB infrastructure (i.e. application server, Oracle Fusion Middleware infrastructure environment, Oracle Services Bus, Extensible Markup Language (XML) Security Gateway).
    2. Maintain and apply DOS Authorized and vendor recommended Operating System (OS) security patches and SOA updated security patches.
    3. Maintain, monitor, and report Oracle SOA Suite backup and recovery.
    4. Increase reusability of IT resources through automation (i.e. Puppet, or Oracle Enterprise Manager or equivalent).
    5. Support integration for new services once developed by development or engineering teams.
    6. Generate reports as requested in support of database/middleware services.
m. Maintain lifecycle of SOPs and KBAs in accordance with CST policies.
n. Perform database and DB infrastructure upgrades and migrations.
o. Deploy and coordinate CA applications and database releases as well as configuration/data changes to central, domestic, and overseas locations.
p. Review and update database scripts provided by other teams in the development/testing phase.
q. Ensure replication is configured and working in accordance with engineering standards.
r. Perform deployments and provide current status and provide a schedule of percent complete, execute and verify Data Definition Language (DDL)/Data Manipulation Language (DDML)/Scripts.
s. Manage and monitor distributed transactions.
    1. Datashare health with partner agencies.
    2. Replication processes/transactions.
    3. Internal to and between data bases, ESB, and applications.

t. Perform proactive and reactive database maintenance, database cleaning, creation, installation, and troubleshooting.
u. Adapt self-healing/corrective actions.
v. Provide support to Application DEV teams, Service Operations, Independent Verification and Validation (IV&V), training, partners, and other Agencies.
    1. Execute various database service accounts password reset process in OpenNet and DMZ sites as defined by CST security teams and CA/CST GTMs (currently this is every 60 days).
    2. Manage database message propagation/queues (i.e. Advanced Queue Message Queue (AQMQ), DMZ, etc.).
    3. Troubleshoot Datashare partner's database connections.
    4. Work with IV&V team in installing special project scripts in development or test environments.
w. Exadata support tasks include, but not limited to:
    1. Standby builds for Replication on Exadata (Production and non-production) machine, proof of concept environment, and Business Intelligence Proof of Concept (BI) POC Environment.
    2. Provide operational input/support on implementation and testing of (OAR to OGG) projects.
    3. Perform PM on Exadata on production and non-production systems, databases, and applications.
    4. Support Secure Shell (SSH) key implementation on Exadata machines (production and non-production).
x. Provide operational input/support to testing and development teams based on engineering/architectural team recommendations.
y. The contractor shall support database security tasks for databases used by legacy, client/server and web-based applications.

C.5.2.7 SUBTASK 7—APPLICATION SUPPORT

The contractor shall provide support for all CA/CST IT systems, web applications, unique imaging and archiving applications, client-server applications and specialized applications supporting multiple functions, and support training for CA/CST technical staff. The contractor is responsible for ensuring all applications meet minimum DOS compliance requirements, and providing proactive and reactive Tier II support services. The contractor shall ensure that all problems/incidents are logged into the Ticket Management System and managed in accordance with the **TTO Section (C.5.2.4.2**) of the TO.

The contractor shall provide support to CA applications including, but not limited to, the following:

a. Legacy CA applications.
b. Modernized ConsularOne applications (including Enterprise Payment System (EPS), Consular Account Management (CAM) system, Consolidated Appointment System, Online Passport Renewal (OPR), and Electronic Consular Record of Birth Abroad (eCRBA).

The contractor shall provide support services for installation/deployment of CA applications; including troubleshooting, diagnosis, evaluation, maintenance, availability, and performance

monitoring. The contractor is responsible for implementing self-learning/self-healing corrective actions to enhance applications. The contractor is responsible for reducing operational down time for critical, scheduled and unscheduled maintenance by accelerating deployments of approved changes/fixes/ or updates.

The contractor shall perform routine application maintenance that includes, but is not limited to the following:

a. Emergency system support/emergency changes.
b. Application updates and patches.
c. Maintain and update passwords in accordance with CA/CST requirements.
d. Maintain, install, remove, and renew application certifications as required.
e. Work with Tier III teams to manage application readiness for Authority to Operate (ATO) or Assessment and Authorization (A&A) process.
f. Provide a migration strategy and project plan for new/additional automated tools as required, if requested by the FEDSIM COR and/or CA/CST GTM.
g. Coordinate, configure and switch production applications from primary instances to standby or DR instances.
h. Troubleshooting, diagnostic and resolution support for CA applications.

The contractor shall ensure that all system components are operational within required availability thresholds. The contractor is required to provide a migration strategy and project plan for new/additional automated tools as required, if requested by the FEDSIM COR and/or CA/CST GTM.

C.5.2.7.1 INSTALLATION/DEPLOYMENT OF APPLICATIONS

The contractor shall perform installation/deployment support of CA supported applications for systems operating across the CA IT global enterprise. CST is moving towards a Continuous Integration Continuous Delivery (CI/CD) approach and or a DevSecOps model. Specific requirements include but are not limited to:

a. Support Deployment Readiness Review (DRR) activities for identified applications as required by the Government.
b. Confirm operational readiness prior to transitioning new applications, or major application upgrades to support.
c. Deploy CA applications and COTS software at operational sites using a DevSecOps or CI/CD tools, as appropriate.
d. Work with other CST installation and support specialists to establish and implement the configuration parameters that optimize operating system performance on customer desktops and servers.
e. Track and report on deployment status of applications.

C.5.2.7.2—SHAREPOINT ADMINISTRATION SUPPORT

The contractor shall provide SharePoint administration support to all CA SharePoint sites. IRM manages the SharePoint infrastructure. (Refer to Section C.3) Support tasks include, but are not limited to:

a. Administer and maintain SharePoint online SharePoint sites.

b. Provide SharePoint support assistance for SharePoint sites, including supporting add-ins and bug fixes using Microsoft FLOW, HTML, jQuery, and Javascript.
c. Create, maintain, and troubleshoot site collections, project sites, lists, and libraries.
d. Review system resources, including Unified Logging System (ULS) and Windows Logs for system health concerns.
e. Monitor permissions and audit logs for governance violations.

C.5.2.8 SUBTASK 8 –ENTERPRISE OPERATIONS CENTER (EOC)

The contractor shall manage an EOC in order to support all Tier II-related assigned incidents. The contractor is responsible for data entry, documenting, tracking, managing and responding to queries regarding the status of any or all problems or requests reported. The contractor shall ensure that all problems/incidents are logged into the Ticket Management System and managed in accordance with the **TTO Section (C.5.2.4.2)** of the TO. CA's current EOC is located onsite at SA-17.

Using the enterprise monitoring capabilities, the contractor is required to:

a. Availability - Monitor infrastructure system availability for all CA locations, coordinating with the IRM Enterprise Network Monitoring Operations Center (ENMOC) to track and resolve issues impacting CA users.
b. Utilization - Monitor infrastructure utilization to ensure the network infrastructure accommodates CA traffic, analyzing utilization trends to proactively request and track upgrades including bandwidth, memory, and storage space. The contractor shall coordinate with other DOS entities and external organizations when required to establish and verify the system operational baseline and utilization.
c. Failures - Track all infrastructure component failures and affecting escalation actions necessary to ensure appropriate support response and within designated time thresholds established. For serious system degradation, the contractor shall ensure management tools are configured with thresholds that will alert the contractor of a potential problem and that a trouble ticket has to be generated for tracking and troubleshooting purposes. The contractor is responsible for providing recommendations to CA/CST for taking action to correct the problem such as infrastructure support or field support.
d. Security - Monitor, analyze, assess, and review audit trails and logs and other information collected for the purpose of searching out system events that may constitute violations of system security.

The contractor shall provide the following, but not limited to:

a. Perform proactive monitoring and respond to incidents, and alerts generated via system/application monitoring SW implemented within the Enterprise Event Management and Monitoring capability.
b. Reallocate systems resources as necessary, optimize systems performance, and recommend additional components to improve overall performance.
c. Maintain account management using RBAC for access to all CA the systems and equipment.
d. Monitor, manage, and optimize system/application performance, availability, and capacity and generate performance reports.

e. Perform system/application diagnostics through the use of Government-provided maintenance tools to ensure availability and to provide an immediate notification of problems to administrators.

C.5.2.9 SUBTASK 9—ENTERPRISE MONITORING

The contractor is required to develop and maintain an enterprise monitoring solution that enables proactive alerting to technical teams as well as integrated dashboards that will provide views into the status of the operational environment. The contractor shall install, maintain, and operate these tools to monitor against established thresholds and provide alerting and reporting to enable proactive management. The contractor is responsible for implementing monitoring solutions to reduce the time, effort, and cost involved with managing and monitoring applications with real-time insight into availability, performance, capacity, and overall health of the environment. The contractor shall track service levels and measure compliance according to DOS, CA, CST, and DS policies and standards.

The enterprise monitoring solution is required to integrate seamlessly and securely with enterprise systems, applications, databases, network connectivity, server/storage infrastructure, and other operational data sources. The enterprise monitoring solution shall cover new systems and applications as well as legacy systems. The enterprise monitoring solution shall interface with the Ticket Management System to automatically create and assign incident tickets detected through monitoring. The enterprise monitoring solution may leverage existing tools or new technology, including but not limited to the following; Oracle Enterprise Manager, Splunk, SolarWinds, VRealize, AppDynamics and Zabbix.

Program-based views will be made available to senior management and technical, user based views will be available for operational staff. High-level views will be used to inform senior CA/CST management on the enterprise health of the environment by providing near-real time availability, capacity, and performance data with the ability to analyze trends and data metrics. Incident ticket information shall be available in the management view to aid CA/CST senior staff in effectively managing problem resolution.

The operational/technical dashboard views and alerting against established thresholds shall be developed at a detailed level to enable highly proactive management of the global CA/IT environment. Alerts will be automatically sent to Tier II and III teams to identify growing problems so that teams may take early action to avoid operational impact.

The enterprise monitoring solution shall meet all policies and mandates for system security, including the ATO. Over the life of the TO, the contractor is responsible for continually identifying opportunities to enhance monitoring with new integration and capabilities.

The contractor is responsible for the collection and analysis of metrics across the CA IT environment. The contractor shall collect, report on, analyze, develop strategies to mitigate problems and improve efficiency and effectiveness and ensure that all efforts are aligned with CA's objectives, mission and goals including a hardened security posture. At a minimum, metrics will be collected to determine the system availability performance, effectiveness of upgrades, costs and return on investment for the introduction of new HW and/or SW.

Contractor support includes but is not limited to:

a. Design, implement, and maintain enterprise monitoring capabilities across the CA IT environment to providing integrated dashboard views and operational alerting to technical teams for action.
b. Maintain the enterprise monitoring environment, maintaining and supporting all monitoring platforms and tools.
c. Establish thresholds for alerting, and coordinate with technical teams to route alerts appropriately.
d. Collect, analyze, and report metrics and develop strategies to mitigate problems and improve efficiency.
e. Provide system metrics to include CPU and memory utilization, system availability, I/O trends, and disk utilization statistics.
f. Provide availability metrics and trending charts to graphically depict information such as uptime, mean downtime, mean time to recovery, and mean time between failures in order to support informed decision-making.
g. Ensure monitoring capabilities are available during scheduled/unscheduled maintenance. Alternate solutions for monitoring must be available if primary solution is unavailable.

C.5.2.10 SUBTASK 10—NETWORK OPERATIONS

The contractor is required to operate and maintain network environments that support connectivity for CA IT systems. This will require coordination with IRM, as the global wide area network provider. The contractor shall ensure that all problems/incidents are logged into the Ticket Management System and managed in accordance with the **TTO Section (C.5.2.4.2**) of the TO.

The contractor shall provide firewall support services to implement and manage both web application firewalls and Next Generation Firewalls (NGFW), including but not limited to: Palo Alto appliances, F5 BIG-IP Application Security Manager and CA API Gateway. The contractor shall troubleshoot firewall issues with IRM firewall teams and facilitate connectivity with other Government Agencies, assist the CA/CST GTM with liaising between CA/CST's and IRM's Firewall Advisory Board for firewall rule submission, and ensure all services are provided in accordance with DOS firewall policies.

The contractor shall provide and maintain network services including, but not limited to:

a. Work with remote CA sites and IRM to establish and maintain WAN connectivity.
b. Configure, maintain, and troubleshoot Transmission Control Protocol/ Internet Protocol (TCP/IP) and other network protocols.
c. Diagram, document, configure, and maintain Local Area Networks (LAN)/Virtual Local Area Networks (VLAN) including rack elevations, LAN wirings, and floor plans.
d. Document and coordinate with the engineering team and/or IRM on static IP assignments.
e. Install, configure, troubleshoot and maintain the following:
    1. Routers, switches, and firewalls per established DOS policies and procedures as required.
    2. Internal network wiring and fiber optic cabling.
    3. LAN using CA approved internetwork operating systems.
    4. Layer two and three devices.

5. Network, network issues, and network monitoring servers, SW (such as SolarWinds, etc.) and HW as required.
6. Remote access devices and SW.
7. Document all existing and potential network problems and outages associated with corrective actions.

f. Analyze network equipment logs to identify trends and problems and maximize network performance through continuous monitoring and troubleshooting.
g. Troubleshoot end-user SSH, Hyper Text Transfer Protocol (HTTP), and other session connection problems.
h. Participate in design review for a new facility or renovations plans.
i. Perform diagnostic testing between network components, among LAN components, and between LAN and WAN components.
j. Perform PM and RM.
k. Recommend configuration changes and network upgrades.
l. Reestablish network connectivity for users during office moves.
m. Report statistical data as requested on LAN utilization.
n. Submit documentation to create Telecommunications Service Request (TSR) for new networking jacks and cabling lines.
o. Monitor utilization of WAN links that support CA remote sites/data center connectivity
p. Coordinate with IRM to plan and execute proactive bandwidth upgrades.
q. Participate in the design, creation, implementation, and troubleshooting of Firewall Rules for networking devices and application communications and connectivity.

C.5.2.11 SUBTASK 11—CONFIGURATION/ CHANGE MANAGEMENT (C/CM)

The contractor shall follow CST's C/CM program for change management and support the Change Management Control Board. Processes shall contain lifecycle C/CM activities in support of all CA/CST infrastructure and applications and shall require collaboration with internal and external stakeholders and across several task areas. The contractor shall prepare a **Configuration/Change Management (C/CM) Plan, (Section F, Deliverable 22)** and update accordingly. The contractor shall ensure the C/CM Plan is developed and maintained using industry best practices (i.e. ITIL). The contractor shall maintain timely accountability of all configuration items and records and coordinate information with incident, problem, change, and release management as required. The contractor is responsible for utilizing automated methods of discovery to reconcile updates with baselines.

Contractor support must include, but is not limited to:

a. Record, track, monitor, and update all configuration items, settings, and all subsequent component configuration changes in the C/CM system.
b. Conduct assessments and actively monitor the computing environment to ensure compliance with what is specified in C/CM requirements and plans.
c. Apply master data management methods to automatically reconcile manual updates and network discovery with the baseline.
d. Document and maintain site topology configuration and changes.
e. Develop, maintain, and communicate configurations and/or changes of configurations in HW/SW and data.

f. Maintain a logical model of all Service Area devices in their relationships by identifying, controlling, maintaining, and verifying installed HW, SW, and documentation (i.e. maintenance contracts).
g. Develop, update, and maintain the existing SOPs and best practices for tools and C/CM activities.
h. Develop, update, and maintain existing and future baseline documentation of each system and application, including designs, build procedures, requirements documents, test procedures, problem reports, SW code, and system knowledge base. Final documentation shall be approved by the Government.

C.5.2.12 SUBTASK 12—CAPACITY AND PERFORMANCE MANAGEMENT

The contractor shall provide capacity management services to ensure the capacity and performance of the CA/CST IT infrastructure meets the demand profiles of CA/CST's evolving business environment in the most cost-effective and timely manner.

The contractor shall provide a **Capacity Management Plan (CMP) (Section F, Deliverable 23**). The CMP details current performance and utilization, future requirements, capacity projections, capacity issues, and plans for improving performance and satisfying business requirements. The CMP must also include the capacity management processes and procedures and identify any financial impacts associated with risk assessments and/or recommendations.

The contractor is required to perform the following key capacity management activities:

a. Define and develop capacity utilization to aid in planning for budgeting purposes to enable expansions of infrastructure.
b. Implement tools that allow for effective capacity monitoring, trending of IT infrastructure, applications, and IT environments.
c. Establish capacity management thresholds to monitor across all systems, applications, databases, and infrastructure.
d. Continually monitor IT resource usage to enable proactive identification of capacity and performance issues.
e. Perform tuning activities to improve IT infrastructure capacity and performance (under the control of change management).
f. Capture trending information and forecast current and future CA/CST IT capacity requirements based on CA/CST IT defined thresholds. Use the information from capacity planning to define and establish thresholds. Ensure data feeds into monitoring systems.

C.5.2.12.1 CAPACITY MANAGEMENT REPORTS

The contractor shall provide capacity management reports and performance reports including but not limited to:

a. Service Performance Information and Reports: reports on the performance.
b. Services Capacity Information and Reports: reports measuring capacity against thresholds.
c. Workload Analysis and Reports: reports providing information about workloads that can be used for enterprise modeling, sizing, and capacity planning.
d. Ad Hoc Capacity and Performance Reports: performance and utilization reports generated on an as-needed basis, typically in response to capacity issues.

e. Forecasts and Predictive Reports: reports used to plan capacity changes and proactively identify potential capacity issues.

C.5.2.13 SUBTASK 13—SECURITY OPERATIONS

The contractor shall work with the CA/CST ISSO group to manage and support security and IA compliance of all CA IT environments. The contractor shall implement a security operations program that considers the selection, design, implementation, test, and operational monitoring of security controls across the operating environments on the production network. The security operations program shall meet all security requirements and be accredited by DOS IRM/IA. The contractor shall document the security controls using the DOS processes and templates. The contractor is required to document and maintain security diagrams, plans, documentation, procedures, policies, logs, , and reports. The contractor is responsible for providing support as required for conducting security tests to validate that required security controls are properly implemented, operate as intended, and produce the desired outcome. The contractor shall fully cooperate with DOS audits, reviews, evaluations, tests, and assessments of contractor systems, processes, and facilities. The contractor shall comply with security controls as specified in NIST SP800-53 Rev 4 (or later), Security and Privacy Controls for Federal Information Systems and Organizations. The contractor is responsible for coordinating with external stakeholders within and outside of DOS in order to coordinate security strategies, initiatives, and incident response/recovery as needed.

C.5.2.13.1 –INFORMATION ASSURANCE (IA) AND COMPLIANCE SUPPORT

The contractor shall perform IA and compliance support services to maintain production system security posture, which includes engineering, implementing, operating, and monitoring. This work shall be completed using the policy and guidelines from the CA/CST ISSO. The ISSO has responsibility for all IA compliance within CA/CST. Activities required under this task area include, but are not limited to:

a. Support for the A&A process (a different team/contractor is responsible for overall coordination and management of the A&A process).
b. Support Plan of Action and Milestone (POA&M) findings develop/implement remediation, as assigned by the CA/CST/ISSO as well as POA&M status reporting.
c. Support the identification, remediation, tracking, management, and/or validation of findings from other sources outside of the A&A process.
d. Maintaining standard configurations in compliance with DOS security standards.
e. Manage security compliance using the Group Policy Object (GPO).
f. Support Enclaving /Network segregation.

The contractor is responsible for maintaining and managing the POA&M for IA findings. A POA&M contains the actions necessary to correct system security weaknesses. The contractor is required to maintain acceptable levels of POA&M grade(s):

a. The contractor shall remediate and close open POA&M items.
b. The contractor shall update open POA&M items monthly.

The contractor is responsible for managing findings from sources other than IA. This may include, but is not limited to; the status of findings as well as coordinating with external organizations. The contractor is responsible for mitigating vulnerabilities in the scope of the

CAEIO contract and advising CA/CST teams and Government stakeholders on how to manage and/or mitigate vulnerabilities and exposures discovered in the environment.

C.5.2.13.2 SECURITY OPERATIONS GUIDES

The contractor shall standardize secure installations guides for the Operating Systems, databases, virtual machines and any other configurable SW as needed. If DS guide exists, the contractor is required to develop a CA configuration guide based on other Federal configuration guides (e.g., Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs)) or industry best practices) for Government approval. The contractor shall baseline configuration guides, following the CA/C/CM process (**Section C.5.2.11 Configuration/Change Management**), and maintains baselines. The contractor is responsible to regularly review all approved baselines to confirm that no changes/updates are required.

The contractor shall notify the CA/CST ISSO of planned HW/SW changes to allow for A&A before deploying into production. The contractor is responsible for ensuring that operating environments meet appropriate security-approved thresholds for sites. The contractor shall comply with DOS patch timeframe requirements in accordance with relevant Notification Bulletins.

C.5.2.13.3 SECURITY OPERATIONS SUPPORT

Security operations support focuses on the operational security administration and Security Information and Event Management (SIEM). The contractor shall support the implementation, configuration, and administration of the SIEM processes and tools in the CA environment. The contractor also is required to support the development, engineering, configuration, implementation, and/or management of security solutions for addressing specific threats, vulnerabilities, or exposures in the environment requested by the Government.

Threat monitoring includes, but is not limited to:

a. Open Source Intelligence Threat (OSINT) monitoring: Collecting information from public sources as well as interagency intelligence and DOS sources outside of CA.
b. Digital Forensics and Analytics: The ability to search across logs on different applications and systems in different time periods based on specific criteria.
c. Incident Identification and Correlation: Identifying common attributes and linking events together into meaningful bundles to identify threats to CA's environment as well as identifying incidents of compromise which may not have been detected by other sources.
d. Incident Response and Recovery: Coordinating the investigation of incidents from all sources as well as supporting investigation, remediation, and recovery activities; as required.
e. Security Posture Assessment/Cyber Hygiene: Responding to reports provided by other bureaus and other Government agencies on vulnerabilities and threats. As requested, the contractor must conduct testing to verify that security solutions intended to mitigate findings in the environment function as intended.
f. Retention: Employing long-term storage of historical data to facilitate correlation of data over time and to provide the retention necessary for compliance requirements.

C.5.2.13.4 PATCH AND SECURITY UPDATE

The contractor shall perform patch management and security update operations support to maintain operating environment compliance, including but not limited to:

a. Provide oversight and periodic review of the patch management process.
b. Deploy and manage all CA patch/security update operations.
c. Perform patch and security update deployment testing.
d. Monitor, report, and remediate all deployment failures within 24 hours.
e. Monitor and report patch and security update compliance for all CA systems weekly.
f. Maintain the CA Patch File Transfer Protocol (FTP) site.
g. Provide weekly, monthly, and/or as requested patch and security update status reports.
h. Comply with DOS rules and regulations governing patch and security update operations.
i. Author and maintain SOPs, policies, and appropriate patch/security documentation including policies detailing patch and security update processes and procedures.
j. Ensure anti-virus tools comply on all devices and monitor, alert, troubleshoot non-compliance incidents.

C.5.3 TASK 3—REDUNDANCY AND DISASTER RECOVERY (DR)

CA/CST services must remain operational and highly available to execute its mission in support of Embassies, Consulates, Passport Agencies and Centers. A robust and proven disaster recovery capability is necessary to support this requirement. The contractor shall develop, manage, and provide support for the enterprise DR program for the CA IT network.

CA/CST has redundancy both within the primary data center at ESOC/West (referred to as "2N") and at a separate DR data center (Modular Data Center) to enable recovery of critical applications, databases and services as needed. Automated failover is in place for some services while SOPs guide manual recovery in other cases. Current 2N and DR capabilities focus on data center based CA services. Recovery options must be developed for domestic Consular offices and overseas posts to ensure the DR Plan **(Section F, deliverable 24)** encompasses the full enterprise.

The contractor shall complete and maintain the CA 2N and DR capabilities to provide continuous improvement and automating failover where possible to achieve faster recovery and more reliable and highly available CA services. The contractor is required to enable seamless switching between the primary and secondary 2N locations to support DR activities and maintenance. The contractor shall enhance and maintain the **DR Plan (Section F, Deliverable 24)** and validate the recovery capabilities through periodic tests. Targeted recovery tests are conducted throughout the year. CCD recovery is tested semi-annually. DR exercises include both partial tests and tabletop exercises.

The contractor shall:

a. Enhance and maintain DR program documentation, including but not limited to a **DR Plan (Section F, Deliverable 24)** and a **Business Impact Analysis (Section F, Deliverable 25**.
b. Maintain the CA/CST Redundancy Chart that tracks recovery options for each application, database and service managed by CA/CST.
c. Coordinate DR tests across the enterprise and document results. CCD DR tests are conducted semi-annually and are considered significant events with pre-planning efforts

beginning weeks in advance of the weekend test. Lessons learned are conducted afterwards to ensure continuous improvement. Other targeted and more limited DR tests are conducted throughout the year, as 2N and MDC2 capabilities are tested.

d. Coordinate with system owners to ensure DR capabilities are maintained as changes are made to systems and environments.
e. Coordinate with owners of new systems to ensure DR requirements are considered and DR plans are made.
f. Support system and facility contingency planning, DR, and testing, as needed to support COOP Planning (Note: providing a DR site is outside the scope of this contract).
g. Assist the Government in coordinating with CA COOP teams to ensure the CA/CST DR Plan and program align with Bureau COOP plans and goals.

C.5.4 TASK 4 –ENGINEERING AND IMPLEMENTATION SERVICES

The contractor shall provide a broad range of HW, network, and COTS SW configuration design and implementation services across the CA IT infrastructure necessary to host, deploy, and integrate systems specified by the Government. This includes the engineering of LANs within data centers and other DOS locations both domestically and abroad.

Operational designs for critical systems shall ensure capabilities to operate in the event of the loss of physical infrastructure within a data center or a broader loss that requires across-Data Center redundancy. The contractor is responsible for providing operational designs that shall require, at a minimum, redundant, synchronized standby infrastructure to enable both active/active and active/passive operations within and/or across multiple hosting environments. The contractor is required to design redundant, synchronized standby infrastructure in a “shared nothing” implementation design, allowing standby systems to be usable in the event of HW or network impacts to production systems.

The contractor shall design operating environments capable of automated switchover or failover with a minimal amount of human intervention. The contractor shall engineer and implement physical data center and server-room configurations and networking within CA enclaves, as well as design and implement network integrations with DOS enterprise networks managed by IRM. The contractor shall develop detailed project plans when implementing new features or capabilities. The contractor is required to update all IT infrastructure documentation to reflect the newly implemented changes.

C.5.4.1 SUBTASK 1—ENGINEERING INFRASTRUCTURE SERVICES

The contractor shall provide engineering services for physical hosting/operating environments for all CA systems, both domestically and abroad. The engineering and design services shall cover physical and virtual Windows and UNIX/Linux Server platforms, the contractor is to install, manage, and maintain DOS compliant server hosting within the data centers as well as other Consular locations. This includes the design and implementation of local infrastructure deployed at all facilities. The hosting environments and operating platforms must enable the necessary computer and storage requirements to support local operations in the event of disconnected or intermittent communications with data center-deployed capabilities. In addition, design solutions must leverage, to the extent possible, converged HW and storage solutions to enable decreased deployment footprints without sacrificing performance or availability.

The contractor is responsible for providing engineering and implementation services for core infrastructure consisting of, but not limited to, the following:

a. Design and implement physical/virtual hosting environments to support CA IT systems. The contractor shall diagrammatically represent layouts of all infrastructure required to support production systems. The contractor shall design all operating environments to conform to all DOS and CA physical and information security requirements.
b. During TO performance review and recommend new equipment and HW/SW requirements for CA approval.
c. During TO performance review and recommend cloud services, where appropriate, for CA approval.
d. Enable the rapid provisioning and deployment of standardized operating environments (e.g., virtual server and virtual network appliance assets) onto the network with automation. Automation shall additionally enable CA to burst capacity as needed during peak loads, but it is required, at a minimum, reduce human intervention and manual processes involved in deploying new virtual assets into production.
e. Support modernization initiatives including but not limited to designing and implementing evolutions to CA infrastructure based on industry best practices, optimization, and modernization to reduce costs and improve services. This includes, but not limited to, transitioning resources from decentralized deployments to centralized data-center-oriented operating environments, migration of systems from physical to virtual operating environments, and use of Federal Risk and Authorization Management Program (FedRAMP) compliant cloud systems. Infrastructure modernization efforts include:
    1. Supporting CA/CST in developing proposals for evaluation by the DOS Cloud Computing Governance Board, and support implementation of off-premise cloud solutions as approved by the Government.
    2. The design and implementation of on premise IaaS and PaaS capabilities, as well as expanded use of containerized deployment strategies (e.g. Docker,). Modernization engineering efforts shall include methods to enable the “portability” of provisioning models, allowing infrastructure and platform templates to be potentially transitioned from on premise hosting environments to FedRAMP compliant cloud systems.
    3. Increased automation to enable the management of server configurations and lockdowns, auditing managed assets to ensure configuration drift is detected and corrected.
    4. Supporting IaaS platforms to enable the rapid provisioning of compute, network, and storage capabilities to support both non-production and production requirements. IaaS capabilities shall be capable of providing self-service provisioning services by authorized users, and establishing operating environments that are conformant to DOS and CA/CST configuration and security template requirements. IaaS-provisioned environments shall be capable of being monitored by the CAEIO-developed enterprise monitoring environment.
    5. Supporting PaaS offerings that enable standardized, application-level templates for core application platforms (e.g. Weblogic, Apache Web Server, IIS, and Oracle database) with defined structures and procedures that enable the deployment of custom application SW into platform containers.

6. Supporting SW-defined infrastructure, including network and storage assets that enable the use of replicated object storage to enable efficient access to resources world-wide.

C.5.4.2 SUBTASK 2 –ENGINEERING IT SERVICES

The contractor shall provide engineering and implementation services used across the CA IT enterprise. The contractor is required to design and implement upgrades and/or enhancements to:

a. Network File Sharing: Server and storage file infrastructure to support distributed high volume data storage and networked file sharing.
b. Active Directory (AD): The CA AD domain to provide authentication and authorization services for CA's organizational units in the NCR and domestic facilities. The contractor is responsible for supporting CA/CST in liaising between CA and IRM for all AD requests and issues.
c. Backups: Backup services for CA servers and systems and data centers. The contractor is required to provide the ability to ship and safeguard backups in a redundant manner off-site from the primary operating environment, maintain the integrity, and perform audit checks of backups. Backup and restoration infrastructure currently includes specialized platforms such as EMC Data Domain and Oracle Zero Data Loss Recovery Appliance.
d. Exchange: Microsoft Exchange clusters (2010 or later) in data center facilities and Exchange servers (2010 or later) at domestic Consular facilities.
e. Domain Name Systems (DNS): The contractor is responsible for coordinating and collaborating, via CA/CST, with IRM to ensure all DNS implementation approaches conform to and integrate with DOS requirements and infrastructure.
f. Dynamic Host Configuration Protocol (DHCP): DHCP scopes and leases for CA.

C.5.4.3 SUBTASK 3 –NETWORK ENGINEERING

The contractor shall perform Network Engineering to support LAN network optimization and standardization at DOS facilities. The contractor shall coordinate through CA/CST with IRM to engineer upgrades to WAN links connecting CONUS and OCONUS Consular facilities. The contractor is responsible for engineering and implementing high availability load balancing, and dynamic service health checks to maximize availability of all public-facing websites in the Public DMZs. In conjunction with IRM, CA/CST's network service provider, the contractor shall engineer, implement, and monitor denial of service detection.

The contractor shall support upgrades required to connect partner agencies to the CA IT network infrastructure. There are approximately 42 external partners. This will include designing enhancements and upgrades to systems for potential future cloud integration/migration.

The contractor is required to perform the following performance-planning-related items:

a. Develop, document and maintain standards and procedures manuals, and performance management procedures that meet CA/CST's requirements.
b. Perform network component tuning to maintain optimum performance in accordance with change management procedures.

C.5.5 TASK 5 -ASSET AND ACQUISITION MANAGEMENT

C.5.5.1 SUBTASK 1 - ACQUISITION SUPPORT

The contractor shall provide acquisition support to include researching alternatives/market research and the preparation of procurement packages for CA/CST's Acquisition Management Office (CA/AQM). Acquisition support includes but is not limited to:

a. Providing detailed specifications, statements of work, and justification documentation.
b. Providing cost estimates in support of Independent Government Cost Estimates (IGCEs).
c. Routing procurement packages through CA/CST for Government approval.
d. Tracking the status of procurement packages with CA/CST and CA/AQM.
e. Reviewing invoices and obtain signed receiving reports from vendors and Government personnel
f. Providing oversight and maintenance of contract files through contract close out
g. Facilitating and preparing file information in response to audits.

In Fiscal Year 2016, CA/CST processed approximately 317 HW/SW procurement requests, ranging from small to multi-million dollar packages. This information is provided as a sample of the contractual documentation required to support this effort.

Additionally, the contractor may be required to procure IT related goods and services for CA/CST in support of the services provided under this TO. In support of this effort, the contractor is responsible for providing and maintaining all of the required documentation to support the procurements completed for this TO **Copies of all Purchase Orders/Purchase Requests/Subcontracts/Professional Services/Maintenance & License Agreements** (**Section F, Deliverable 26**). The contractor is responsible for ensuring that proof of entitlements, warranties, and other artifacts are registered in CA/CST's name and maintained in accordance with the agreements. The contractor may be required to purchase the following (this list is not all inclusive):

a. HW
b. SW
c. Peripherals
d. Supplies and parts in support of Card Printer maintenance (**Section C.5.2.5.2.1**)
e. License and maintenance agreements
f. Warranties and/or warranty extensions
g. Professional services

C.5.5.2 SUBTASK 2 –ASSET MANAGEMENT

The contractor shall maintain a complete and accurate inventory of all assets and licenses acquired and/or deployed into production environments within CA (management of the CST warehouse is outside the scope of this TO). There are just under 41,000 units of HW according to the inventory report. The inventory list shall be made available to the Government.

The contractor is required to create and maintain an official record of asset inventory (HW or SW) outside of CA's Integrated Logistics Management System (ILMS). This includes tracking and decommissioning of inventory distributed to CA/CST personnel and the location of inventory. The contractor is responsible for completing all in-processing, including opening boxes, completing any required acceptance testing (customary for COTS/GOTS items),

assessing and coordinating with vendors to replace items damaged during shipping, and ensuring conforming assets are stored in a secure facility within two business days. The contractor shall notify CA/CST of any discrepancies within one business day.

a. Asset Tracking: The contractor is required to provide HW and SW asset management services throughout the asset's lifecycle. The contractor shall complete reconciliation activities; report generation, trend analysis, periodic inventory reviews, inventory reconciliation; and assist in asset management operational compliance reviews, and data maintenance for COTS SW licenses. The contractor is responsible for assigning barcodes for the NCR equipment, in coordination with the General Service Division (GSD) within CA. The contractor is responsible for working closely with SD staff to ensure that actions related to equipment provisioning are maintained appropriately.
b. HW/SW Changes: The contractor is required to plan for and coordinate HW/SW changes with Change Management to ensure the approved standard is maintained.
c. Provisioning Equipment: The contractor is required to coordinate with the SD and other support groups and/or on-site System Administration (SA) support to provision equipment to users. The contractor is responsible for responding to requests for HW or SW. Provisioned equipment shall include agency assets and licenses acquired or deployed into production environments including but not limited to, desktop/laptop computers, printers, copiers, AV equipment (projectors, portable screens, data, monitors); network equipment (servers, routers), portable hard drives, SW, and local consumables.
d. Inventory management: The contractor is required to track inventory outside of the ILMS. If equipment is broken and requires replacement (break/fix), the contractor shall verify warranty information within the DOS warranty tracking system. If replacement equipment is required, the contractor is responsible for coordinating with its Acquisition Support to procure replacement parts and maintain required stock thresholds. The contractor shall manage inventory deploying and operating in all domestic CA facilities. The contractor is required to coordinate with third-party logistics providers on the shipment/receiving/storing of equipment to/from CST warehouses or other DOS facilities.
e. Media Sanitation: Hard drives and other data holding devices, whether part of a workstation, laptop, or stand-alone, shall be processed for disposal in accordance with DOS CIO procedures.
f. Semi-Annual SW Inventory: The contractor shall conduct a semi-annual inventory of all SW assets and develop a formal status **Semi-Annual Inventory Report (Section F, Deliverable 27).** The inventory report should include all assets regardless of warranty status. The inventory report should identify the following: all SW assets currently installed throughout the environment; SW assets legally purchased; SW assets installed not purchased; SW assets (over/under) subscribed based upon purchase history and installation base; and recommendations to purchase additional licenses or to de-install SW not being utilized since the previous reporting period.
g. Semi-Annual HW Inventory Report: The contractor is responsible for conducting a bi-annual inventory of all HW assets and develop a formal **Semi-Annual Inventory Status Report (Section F, Deliverable 28).** The contractor shall perform due diligence and provide the status on HW assets not identified during bi-annual inventory. The inventory report should include all assets regardless of warranty status. The inventory report should identify the following: all HW assets successfully inventoried with the location of the

assets verified; all HW assets not verified during the inventory; assets marked as surplus since the last reporting period; assets lost since the last reporting period; and identify assets traded-in, exchanged, or returned to the vendor since the last reporting period.

h. Maintain SW Library: The contractor shall maintain the CA/CST's centralized SW library to ensure that media exists for each software asset; proof of entitlement and SW restrictions or usage rights exists for each SW asset; proof of maintenance exists for each software asset; media installation or other security codes to install SW assets exists for each software asset; and all records and media are duplicated in an offsite location for DR purposes.

The contractor shall issue encrypted Universal Service Bus (USB) thumb drives to CA customers and issue HW/SW to other contractors within NCR as approved by the Government. (The issuance of HW will include HW/SW provided to CST Desktop Support and IRM technicians in support of staff located in DOS facilities.)

C.5.5.3 SUBTASK 3 –WARRANTY MANAGEMENT

The contractor shall track all HW and SW warranty information outside of CA's ILMS system; however, warranty management within the ILMS may be required in the future performance of this TO. A current warranty list will be provided in accordance with **Section H.3.** Warranty Management includes monitoring existing warranties and ensuring appropriate warranties for all equipment purchases to meet the Government's needs. The contractor shall provide early notification and appropriate resource advice of upcoming expirations of maintenance, warranty, or license agreements within 30, 60, 90, and180 days. The contractor is responsible for coordinating with the license renewal and tracking on potential warranty expirations that may impact the license renewal process.

C.5.5.4 SUBTASK 4 –LICENSE MANAGEMENT AND TRACKING SUPPORT

In coordination with CA/CST, the contractor shall develop and provide **License Management & Tracking Procedures** (**Section F, Deliverable 29**) for each SW license and/or maintenance classification. A current list of all licenses will be provided in accordance with **Section H.3.** All changes to the renewal and tracking procedures must be approved by CA/CST. The contractor shall ensure that all SW license transfers (e.g., the transfer of licenses during a device refresh and/or the transfer of licenses during resource attrition) are reflected in the Asset Management System (AMS) within two business days of the completion of the transfer. Each license resident in the AMS must be flagged for renewal six months and three months prior to expiration. Following the six-month renewal notification and prior to ordering new SW licenses and/or maintenance, the contractor shall confirm the renewal terms and SW license needs with CA/CST. No sooner than six months before the software license and/or maintenance expiration date, the contractor shall renew the software licenses and/or maintenance with CA/CST and FEDSIM COR approval.

The contractor shall understand and document the penalties for early renewal. The renewal process shall be just-in-time and include no overlap cost of the SW licenses and/or maintenance. The contractor shall update the AMS with the new SW license and/or maintenance expiration date(s). The contractor is responsible for monitoring and maintaining the equipment (HW/SW) license data repository that records and tracks all information pertinent to the lifecycle

maintenance of the product. This includes the vendor name, SW name and version, number of authorized users and/or devices covered, licensing fees, HW age, and commencement and expiration dates. The contractor is responsible for running periodic checks of the equipment installed on the networks to ensure that the appropriate licenses are assigned. SW and HW without the appropriate license would require permission to operate.

C.5.5.5 SUBTASK 5 –DEVICE RETIREMENT SUPPORT

In collaboration with CA/CST, the contractor shall follow DOS procedures for and perform device retirements. Recommendations shall be provided to the CA/CST GTM should changes to this documentation be deemed necessary. The Government will provide sanitation tools, and the contractor shall conduct the sanitization and final disposition of media. The contractor shall perform inventory control for all decommissioned equipment.

This page intentionally left blank.

E.1 PLACE OF INSPECTION AND ACCEPTANCE

Inspection and acceptance of all work performance, reports, and other deliverables under this TO will be performed by FEDSIM COR and the CA/CST GTM. Inspection and acceptance may take place at the GSA Headquarters (1800 F Street, NW, Washington, D.C.) or the DOS Headquarters location.

E.2 SCOPE OF INSPECTION

All deliverables will be inspected for content, completeness, accuracy, and conformance to TO requirements by the FEDSIM COR and CA/CST GTM. Inspection may include validation of information or SW through the use of automated tools, testing, or inspections of the deliverables, as specified in the TO. The scope and nature of this inspection will be sufficiently comprehensive to ensure the completeness, quality, and adequacy of all deliverables.

The Government requires a period NTE 15 workdays after receipt of final deliverable items for inspection and acceptance or rejection.

E.3 BASIS OF ACCEPTANCE

The basis for acceptance shall be compliance with the requirements set forth in the TO and relevant terms and conditions of the contract. Deliverable items rejected shall be corrected in accordance with the applicable clauses.

The final acceptance will occur when all discrepancies, errors, or other deficiencies identified in writing by the Government have been resolved, through documentation updates, program correction, or other mutually agreeable methods.

Reports, documents, and narrative-type deliverables will be accepted when all discrepancies, errors, or other deficiencies identified in writing by the Government have been corrected.

If the draft deliverable is adequate, the Government may accept the draft and provide comments for incorporation into the final version.

All of the Government's comments on deliverables shall either be incorporated in the succeeding version of the deliverable, or the contractor shall explain to the Government's satisfaction why such comments should not be incorporated.

If the Government finds that a draft or final deliverable contains spelling errors, grammatical errors, or improper format, or otherwise does not conform to the quality assurance requirements stated within this TO, the document may be rejected without further review and returned to the contractor for correction and resubmission. If the contractor requires additional Government guidance to produce an acceptable draft, the contractor shall arrange a meeting with the FEDSIM COR.

E.4 DRAFT DELIVERABLES

The Government will provide written acceptance, comments, and/or change requests, if any, within 15 workdays (unless specified otherwise in **Section F**) from Government receipt of the draft deliverable. Upon receipt of the Government comments, the contractor shall have ten workdays to incorporate the Government's comments and/or change requests and to resubmit the deliverable in its final form.

E.5 WRITTEN ACCEPTANCE/REJECTION BY THE GOVERNMENT

The FEDSIM CO or FEDSIM COR will provide written notification of acceptance or rejection (**Section J, Attachment N Template**) of all final deliverables within 15 workdays (unless specified otherwise in **Section F**). All notifications of rejection will be accompanied with an explanation of the specific deficiencies causing the rejection.

E.6 NON-CONFORMING PRODUCTS OR SERVICES

Non-conforming products or services will be rejected. Deficiencies shall be corrected, by the contractor, within ten workdays of the rejection notice. If the deficiencies cannot be corrected within ten workdays, the contractor shall immediately notify the FEDSIM COR of the reason for the delay and provide a proposed corrective action plan within ten workdays.

If the contractor does not provide products or services that conform to the requirements of this TO, the Government will document the issues associated with the non-conforming products or services in the award fee determination report, and there will be an associated impact to the award fee earned.

F.1 PERIOD OF PERFORMANCE

The period of performance for this TO is one-year base period and six, one-year option periods.

Base Period:	December 18, 2019 – December 17, 2020
First Option Period:	December 18, 2020 – December 17, 2021
Second Option Period:	December 18, 2021 – December 17, 2022
Third Option Period:	December 18, 2022 – December 17, 2023
Fourth Option Period:	December 18, 2023 – December 17, 2024
Fifth Option Period	December 18, 2024 – December 17, 2025
Sixth Option Period	December 18, 2025 – December 17, 2026

F.2 PLACE OF PERFORMANCE

The primary place of performance shall be the CA Headquarters location in the National Capital Region (NCR/ SA-17); located at 600 19th ST. NW, Washington, D.C as described in H.2.2. The contractor shall provide a site within 30 miles of the DOS CA/CST Headquarters (NCR/SA-17), commensurate with the contractors' proposed solution. The contractor's site shall meet all the requirements of Section H.4.2. Long-distance travel may be required to provide temporary support for global CA/CST sites.

F.3 TASK ORDER (TO) SCHEDULE AND MILESTONES

The following schedule of milestones will be used by the FEDSIM COR to monitor timely progress under this TO.

The following abbreviations are used in this schedule:

DEL: Deliverable
IAW: In Accordance With
NLT: No Later Than
TOA: Task Order Award

Deliverables are due the next Government workday if the due date falls on a holiday or weekend.

Data Rights Clause - Abbreviations in the Gov't Rights column of the table below shall be interpreted as follows:

UR: Unlimited Rights, per FAR 27.404-1(a) and 52.227-14

For SW or documents that may be either proprietary COTS or custom, RS/LD rights apply to proprietary COTS SW or documents and UR rights apply to custom SW or documents. The Government asserts UR rights to open source COTS SW. Any collateral agreements (within the meaning of FAR 52.227-14) proposed for data, regardless of the type of rights offered, shall be subject to the requirements of TO **Section H.12.1 and H.12.2**. For purposes of the foregoing, the terms "collateral agreement," "Supplier Agreement," and "Commercial Supplier Agreement" have the same meaning.

The Government does not assert any rights to management SW tools if the contractor does not plan to charge the Government directly for that tool and does not propose that the Government will own or use that tool.

SECTION F – DELIVERIES OR PERFORMANCE

The contractor shall deliver the deliverables listed in the following table on the dates specified:

DEL. #	MILESTONE/ DELIVERABLE	TOR REFERENCE	DATE OF COMPLETION/ DELIVERY	GOV'T RIGHTS
	Project Start (PS)		Within 15 Days of TOA	N/A
01	Program Kick-Off Meeting	C.5.1.1	Within 25 days after TOA	UR
02	Program Kick-Off Meeting Agenda	C.5.1.1	At least three workdays prior to the Kick-Off Meeting	UR
03	Program Kick-Off Meeting Minutes	C.5.1.1	At least three workdays after the Kick-Off Meeting	UR
04	Financial Kickoff Meeting	C.5.1.1	During the Program Kick-Off Meeting	UR
05	Contract Status Report (CSR)	C.5.1.2	Monthly, 20th Day of the Month	UR
06	Earned Value Management (EVM) Plan	C.5.1.1, C.5.1.3, H.9	The EVM Plan is due at the Kick off meeting.	UR
07	Weekly Activity Report (WAR)/ Project Status Report (PSR)	C.5.1.4	Weekly for WAR, every other week for PSR	UR
08	Draft Program Management Plan (PMP)	C.5.1.5	Due at Program Kick-Off Meeting	UR
09	Final Program Management Plan (PMP)	C.5.1.5	10 workdays after receipt of Government comments	UR
10	Program Management Plan Updates (PMP)	C.5.1.5	As project changes occur, no less frequently than annually	UR
11	Project Plan	C.5.1.6	Every other week	UR
12	Project Plan Updates	C.5.1.6	Every other week	UR
13	Trip Report(s)	C.5.1.7	As requested, due within 10 workdays following completion of each trip	UR
14	Final Quality Management Plan	C.5.1.5, C.5.1.8	Due 45 workdays after TOA	UR
15	Quality Management Plan (QMP) Updates	C.5.1.1 C.5.1.8	Update annually or as needed.	UR
16	Transition-In Plan	C.5.1.1 C.5.1.9	Within 27 work days after TOA	UR
17	Transition-Out Plan	C.5.1.10	30 Days After Exercising Option Period 2 Update Annually and quarter during the final Option Period	UR
18	Quarterly Spend Plan	C.5.1.12	Quarterly	UR

DEL. #	MILESTONE/ DELIVERABLE	TOR REFERENCE	DATE OF COMPLETION/ DELIVERY	GOV'T RIGHTS
19	Knowledge Management Plan	C.5.2.1	Initial plan due 90 days after Program Kick-Off Meeting Revisions are required, as needed	UR
20	Notification Plan	C.5.2.4.3	Initial plan due 90 days after Program Kick-Off meeting, revisions required as requirements change	UR
21	PM/RM Plan (Card Printers)	C.5.2.5.2.1	114 days after Project Start, Annual Updates	UR
22	Configuration/Change Management Plan (C/CM)	C.5.2.9	120 days after Project Start	UR
23	Capacity Management Plan	C.5.2.10	125 days after Project Start; Semi-Annual Updates	UR
24	Disaster Recovery (DR) Plan	C.5.3	6 Months after TOA; Updates Annually or as needed	UR
25	Business Impact Analysis	C.5.3	6 Months after TOA; Updates Annually or as needed	UR
26	Copies of all Purchase Orders /Purchase Requests/Subcontracts/Professional Services/ Maintenance & License Agreements	C.5.5.1	10 WD after the end of the Month	UR
27	Semi-Annual Inventory Report	C.5.5.2	Semi-Annually	UR
28	Semi-Annual Inventory Status Report	C.5.5.2	Every June and December	UR
29	License Management and Tracking Procedures	C.5.5.4	64 Days after TOA	UR
30	Copy of TO (initial award and all modifications)	F.4	Within 10 workdays of award	UR
31	IBR	H.9	As needed.	UR

The contractor shall mark all deliverables listed in the above table to indicate authorship by contractor (i.e., non-Government) personnel; provided, however, that no deliverable shall contain any proprietary markings inconsistent with the Government's data rights set forth in this TO. The Government reserves the right to treat non-conforming markings in accordance with subparagraphs (e) and (f) of the FAR clause at 52.227-14.

F.4 PUBLIC RESEASE OF CONTRACT DOCUMENTS REQUIREMENT

The contractor agrees to submit, within ten workdays from the date of the FEDSIM CO's execution of the initial TO, or any modification to the TO (exclusive of Saturdays, Sundays, and Federal holidays), a Portable Document Format (PDF) file of the fully executed document with

all proposed necessary redactions, including redactions of any trade secrets or any commercial or financial information that it believes to be privileged or confidential business information, for the purpose of public disclosure at the sole discretion of GSA (**Section F, Deliverable 29)**. The contractor agrees to provide a detailed written statement specifying the basis for each of its proposed redactions, including the applicable exemption under the Freedom of Information Act (FOIA), 5 United States Code (U.S.C.) § 552, and, in the case of FOIA Exemption 4, 5 U.S.C. § 552(b) (4), shall explain why the information is considered to be a trade secret or commercial or financial information that is privileged or confidential. Information provided by the contractor in response to the contract requirement may itself be subject to disclosure under the FOIA. Submission of the proposed redactions constitutes concurrence of release under FOIA.

GSA will carefully consider the contractor's proposed redactions and associated grounds for nondisclosure prior to making a final determination as to what information in such executed documents may be properly withheld.

F.5 DELIVERABLES MEDIA

The contractor shall deliver all electronic versions by electronic mail (email) and removable electronic media, as well as placing in the DOS' designated repository. The following are the required electronic formats, whose versions must be compatible with the latest, commonly available version on the market.

a. Text	Microsoft (MS) Word, Google Docs, PDF
b. Spreadsheets	MS Excel, Google Sheets
c. Briefings	MS PowerPoint, Google Slides
d. Drawings	MS Visio, Google Drawings
e. Schedules	MS Project, Smartsheet

F.6 PLACE (S) OF DELIVERY

Copies of all deliverables shall be delivered to the FEDSIM COR at the following address:

GSA FAS AAS FEDSIM
ATTN: Meaghan Hakala, COR (QF0B)
1800 F Street, NW
Washington, D.C. 20405
Telephone: (202) 297-4598
Email: meaghan.hakala@gsa.gov

Copies of all deliverables shall also be delivered to the CA/CST GTM.

F.7 NOTICE REGARDING LATE DELIVERY/ PROBLEM NOTIFICATION REPORT (PNR)

The contractor shall notify the FEDSIM COR via a **Problem Notification Report (PNR)** (**Section J, Attachment O**) as soon as it becomes apparent to the contractor that a scheduled delivery will be late. The contractor shall include in the PNR the rationale for late delivery, the expected date for the delivery, and the project impact of the late delivery. The FEDSIM COR will review the new schedule and provide guidance to the contractor. Such notification in no way limits any Government contractual rights or remedies including, but not limited to, termination.

G.1 CONTRACTING OFFICER'S REPRESENTATIVE (COR)

The FEDSIM CO appointed a FEDSIM COR in writing through a **COR Appointment Letter** (**Section J, Attachment P**). The FEDSIM COR will receive, for the Government, all work called for by the TO and will represent the FEDSIM CO in the technical phases of the work. The FEDSIM COR will provide no supervisory or instructional assistance to contractor personnel.

The FEDSIM COR is not authorized to change any of the terms and conditions, scope, schedule, and price of the Contract or the TO. Changes in the scope of work will be made only by the FEDSIM CO by properly executed modifications to the Contract or the TO.

G.1.1 CONTRACT ADMINISTRATION

Contracting Officer:

Nydia Roman-Albertorio
GSA FAS AAS FEDSIM (QF0B)
1800 F Street, NW
Washington, D.C. 20405
Telephone: 202-285-9530
Email: nydia.roman-albertorio@gsa.gov

Contracting Officer's Representative:

Meaghan Hakala
GSA FAS AAS FEDSIM (QF0B)
1800 F Street, NW
Washington, D.C. 20405
Telephone: 202-297-4598
Email: meaghan.hakala@gsa.gov

Alternate Contracting Officer's Representative:

Sandy Greenwell
GSA FAS AAS FEDSIM (QF0B)
1800 F Street, NW
Washington, D.C. 20405
Telephone: 703-589-2564
Email: sandy.greenwell@gsa.gov

CA/CST Government Technical Monitor (GTM):

Sandy Kunz
DOS CA/CST
600 19th Street, NW
Washington, D.C. 20036
Telephone: (202) 485-7818
Email: KunzSM@state.gov

CA/CST Alternate Government Technical Monitor (GTM):

Hetal Doshi
DOS CA/CST
600 19th Street, NW
Washington, D.C. 20036

Telephone: (202) 615-8838
Email: DoshiHJ@state.gov

G.2 INVOICE SUBMISSION

The contractor shall submit Requests for Payments in accordance with the format contained in General Services Administration Acquisition Manual (GSAM) 552.232-25, PROMPT PAYMENT (NOV 2009), to be considered proper for payment. In addition, the following data elements shall be included on each invoice:

Task Order Number: 47QFCA-20-F-0015
Paying Number: 21436776
FEDSIM Project Number: 47QFCA-19-S-0016
Project Title: CAEIO

The contractor shall submit invoices as follows:

The contractor shall utilize FEDSIM's electronic Assisted Services Shared Information System (ASSIST) to submit invoices. The contractor shall manually enter CLIN charges into Central Invoice Services (CIS) in the ASSIST Portal. Summary charges on invoices shall match the charges listed in CIS for all CLINs. The contractor shall submit invoices electronically by logging onto the following link (requires Internet Explorer to access the link):

https://portal.fas.gsa.gov

Log in using your assigned Identification (ID) and password, navigate to the order against which you want to invoice, click the Invoices and Acceptance Reports link in the left navigator, and then click the Create New Invoice button. By utilizing this method, no paper copy of the invoice shall be submitted to GSA FEDSIM or the GSA Finance Center. The contractor shall provide invoice backup data, as an attachment to the invoice, in accordance with the contract type, including detail such as labor categories, rates, and quantities of labor hours per labor category. The FEDSIM COR may require the contractor to submit a written "hardcopy" invoice with the client's certification prior to invoice payment. A paper copy of the invoice is required for a credit.

The contractor is certifying, by submission of an invoice in the CIS, that the invoice is correct and proper for payment.

If there are any issues submitting an invoice, contact the Assisted Acquisition Services Business Systems (AASBS) Help Desk for support at 877-472-4877 (toll free) or by email at AASBS.helpdesk@gsa.gov.

G.3 INVOICE REQUIREMENTS

The contractor shall submit a draft copy of an invoice backup in Excel to the FEDSIM COR and CA/CST GTM for review prior to its submission to ASSIST. The draft invoice shall not be construed as a proper invoice in accordance with FAR 32.9 and GSAM 532.9. Receipts shall be provided on an as-requested basis.
The final invoice is desired to be submitted within six months of project completion. Upon project completion, the contractor shall provide a final invoice status update monthly.

Regardless of contract type, the contractor shall report the following metadata:

a. GWAC Number
b. Task Order Award Number (NOT the Solicitation Number)
c. Contractor Invoice Number
d. Contractor Name
e. POC Information
f. Current period of performance
g. Amount of invoice that was subcontracted

The amount of invoice that was subcontracted to a small business shall be made available upon request.

G.3.1 COST-PLUS-AWARD-FEE (CPAF) CLINs (FOR LABOR)

The contractor may invoice monthly on the basis of cost incurred for the CPAF CLINs. The invoice shall include the period of performance covered by the invoice (all current charges shall be within the active period of performance) and the CLIN number and title. All hours and costs shall be reported by CLIN element (as shown in Section B), by contractor employee, and shall be provided for the current billing month and in total from project inception to date. The contractor shall provide the invoice data in spreadsheet form with the following detailed information. The listing shall include separate columns and totals for the current invoice period and the project to date.

a. Employee name (current and past employees).
b. Employee company.
c. Exempt or non-exempt designation.
d. Employee Alliant 2 labor category.
e. Current monthly and total cumulative hours worked.
f. Direct Labor Rate.
g. Effective hourly rate (e.g., cumulative costs/cumulative hours).
h. Current approved billing rate percentages in support of costs billed.
i. Itemization of cost centers applied to each individual invoiced.
j. Itemized breakout of indirect costs (e.g., Fringe, Overhead (OH), General and Administrative (G&A) burdened costs for each individual invoiced (rollups are unacceptable)).
k. Any cost incurred not billed by CLIN (e.g., lagging costs).
l. Labor adjustments from any previous months (e.g., timesheet corrections).
m. Contractor will provide comments when there is a variance of the Direct Labor Rate on a single invoice 10 percent or higher when compared to the Year-to-Date Direct Labor Rate.

All cost presentations provided by the contractor in Excel shall show indirect charges itemized by individual with corresponding indirect rates with cost center information. The invoice detail shall be organized by CLIN.

The contractor may invoice for fee after accepting the modification which includes the award fee determination and any corresponding deobligation of unearned fee. See the **AFDP in Section J, Attachment C** for additional information on the award fee determination process.

When the Incurred Cost method is used to determine the Award Fee Pool Allocation for an Award Fee period, the incurred cost shall be calculated using approved provisional billing rates as established by the cognizant Government auditor, in accordance with FAR 42.704. Approved provisional billing rates shall not be adjusted for the purpose of accumulating incurred costs and calculating the Award Fee Pool Allocation.

G.3.1.1 ADDITIONAL INVOICE REQUIREMENTS FOR ADMINISTRATIVE ODC COVID-19 CLIN ASSOCIATED WITH SECTION 3610 OF THE CARES ACT

a. All costs associated with the CARES Act 3610 relief ODC CLIN shall be segregated onto a separate tab in the invoice.

b. The contractor shall include all relevant contract information, place of performance, affected employee, leave status with supporting documentation of that status, leave duration, and the dollar amount of costs reimbursed pursuant to Section 3610.

c. The contractor shall certify with each invoice that it is not pursuing Section 3610 reimbursement on costs for which the contractor is otherwise entitled to relief, credit or offset under other parts of the CARES Act (Pub. L. 116-136), Division G of the Families First Coronavirus Response Act (Pub. L. 116–127) or any other credit allowed by the laws of any jurisdiction to which the contractor may be entitled that is specifically identifiable with the public health emergency declared on January 31, 2020 for COVID–19. This certification is required regardless of whether the contractor is in actual receipt of or has properly effectuated the accrual of such other relief in its accounting systems, or has properly pursued such relief at the time of invoice submission.

d. The contractor shall certify with each invoice that costs incurred in the payment of leave, including sick leave, to any employee for which reimbursement is sought under Section 3610 is not for costs that would otherwise be appropriately incurred in the ordinary course of its business.

G.3.2 TOOLS AND OTHER DIRECT COSTS (ODCs)

The contractor may invoice monthly on the basis of cost incurred for the Tools and ODC CLINs. The invoice shall include the period of performance covered by the invoice and the CLIN number and title. In addition, the contractor shall provide the following detailed information for each invoice submitted, as applicable. Spreadsheet submissions are required.

a. Tools and/or ODCs purchased
b. Request to Initiate Purchase (RIP) or Consent to Purchase (CTP) number or identifier
c. Date accepted by the Government
d. Associated CLIN
e. Project-to-date totals by CLIN
f. Cost incurred not billed by CLIN
g. Remaining balance of the CLIN

All cost presentations provided by the contractor shall also include any indirect costs applied with the associated cost center information.

G.3.2 TRAVEL

Contractor costs for travel will be reimbursed at the limits set in the following regulations (see FAR 31.205-46):

a. Federal Travel Regulation (FTR) - prescribed by the GSA, for travel in the contiguous U.S.
b. Joint Travel Regulations (JTR) Volume 2, Department of Defense (DoD) Civilian Personnel, Appendix A - prescribed by the DoD, for travel in Alaska, Hawaii, and outlying areas of the U.S.
c. Department of State Standardized Regulations (DSSR) (Government Civilians, Foreign Areas), Section 925, "Maximum Travel Per Diem Allowances for Foreign Areas" - prescribed by the DOS, for travel in areas not covered in the FTR or JTR.

The contractor may invoice monthly on the basis of cost incurred for cost of travel comparable with the FTR/DSSR. The invoice shall include the period of performance covered by the invoice, the CLIN number and title. Separate worksheets, in MS Excel format, shall be submitted for travel.

CLIN/Task Total Travel: This invoice information shall identify all cumulative travel costs billed by CLIN/Task. The current invoice period's travel details shall include separate columns and totals and include the following:

a. Travel Authorization Request number or identifier, approver name, and approval date
b. Current invoice period
c. Names of persons traveling
d. Number of travel days
e. Dates of travel
f. Number of days per diem charged
g. Per diem rate used
h. Total per diem charged
i. Transportation costs
j. Total charges
k. Explanation of variances exceeding ten percent of the approved versus actual costs
l. Indirect handling rate

All cost presentations provided by the contractor shall also include OH charges and G&A charges in accordance with the contractor's Defense Contract Audit Agency (DCAA) cost disclosure statement.

G.4 TASK ORDER (TO) CLOSEOUT

The Government will unilaterally close out the TO no later than six years after the end of the TO period of performance if the contractor does not provide final DCAA rates by that time.

H.1 KEY PERSONNEL

The following are the minimum personnel who shall be designated as "Key." The Government does not intend to dictate the composition of the ideal team to perform on this TO.

a. Program Manager (PgM)
b. Service Center Manager
c. Infrastructure Support Manager
d. Database Support Manager
e. Application Support Manager
f. Network Operations Manager
g. Enterprise Operations Center (EOC) Manager
h. Engineering and Implementation Manager
i. Acquisition and Asset Manager
j. Security Operations Manager

The Government desires that Key Personnel be assigned for the duration of the TO.

H.1.1 PROGRAM MANAGER (PGM)

The contractor shall identify a full-time, single PgM, by name, to serve as the Government's primary POC. The PgM shall be responsible for the overall execution and success of this TO and to provide overall leadership, management, direction, and guidance for all contractor personnel assigned to the TO. The PgM is ultimately responsible for the quality and efficiency of the TO, to include both technical issues and business processes. The PgM shall be readily available to respond to CA/CST's questions, concerns, and comments. This PgM shall be an employee of the prime contractor. This PgM shall have the authority to commit the contractor's organization and make decisions for the contractor's organization in response to Government issues, concerns, questions, and comments, as well as be proactive in alerting the Government to potential contractual or programmatic issues including situations that may comprise the contractor's ability to provide services.

It is required that the PgM has the following qualifications:

a. Possesses a current Project Management Institute Project Management Professional (PMI/PMP) certification.
b. Demonstrated experience with IT Service Delivery using an ITIL/ITSM framework similar in size, scope, and complexity to the requirements of this TO.
c. A minimum of seven years of management experience with a program similar in dollar value, size, scope, and complexity to the requirements of this TO.
d. Demonstrated experience with Earned Value Management on projects of a similar size, scope, and complexity to this TO.
e. Demonstrated experience managing and leading geographically dispersed operations and engineering staff of varying skill levels, in a project environment similar in size and scope as this TO.
f. Possesses a Top Secret clearance.

It is desired that the PgM has the following qualifications:

a. Demonstrated experience implementing service level agreements and performance metrics on a contract.
b. Demonstrated experience with the Federal procurement process and familiarity with the administration of cost-type contracts.
c. Demonstrated experience with the SDLC process, SAFe Agile principles/ methodologies and experience modernizing the processes procedures and application support environment toward CI/CD or DevSecOps approach.

H.1.2 SERVICE CENTER MANAGER

The Service Center Manager shall be responsible for the total management of the Service Center, including SD, Desktop Support, incident and IT service request management and tracking, ticket escalation, communications and notifications, mobile services support, management of knowledge-based articles and SOPs. The Service Center Manager shall be responsible for overseeing SD personnel, responsible for total ticket ownership (from generation through completion) of service requests within the enterprise ticket management system, and the ACD. The Service Center Manager shall ensure users receive efficient and timely Tier 0, Tier 1 and Tier II Desktop support to ensure that service levels are achieved in line with the TO and ensure customer expectations are met or exceeded. The Service Center Manager shall be responsible for improving, optimizing, standardizing, and streamlining customer support processes that yield improvements in customer satisfaction.

It is required that the Service Center Manager has the following qualifications:

a. Possesses an ITIL Foundation Level Certification - (or higher).
b. A minimum of seven years of technical experience managing, maturing, and modernizing a 24x7x365 Service Desk for geographically dispersed users with end-to-end service delivery, similar in size, scope, and complexity to this TO.
c. Demonstrated experience implementing and managing Service Center communications, to include reporting, and experience with strategic and operational planning.
d. Possesses a Secret clearance.

It is desirable that the Service Center Manager has the following qualifications:

a. Possesses a current Help Desk Institute Support Center Manager (HDI-SCM) certification.
b. Demonstrated experience implementing, managing, and modernizing successful Tier 0 services and reporting.

H.1.3 INFRASTRUCTURE SUPPORT MANAGER

The Infrastructure Support Manager has broad responsibility for infrastructure operations and systems administration of platforms installed globally supporting all CA systems and services. This includes management of infrastructure operations and maintenance within the domestic data centers, domestic Consular locations, and overseas at posts. The Infrastructure Support Manager shall ensure the operation of the enterprise meets defined infrastructure service levels and serves as the contractor's service owner for infrastructure service solutions. The Infrastructure Support Manager shall oversee operations and technical teams at multiple geographically dispersed data centers comprised of varied infrastructure, including converged server/storage solutions, at the domestic consular offices and overseas posts. The Infrastructure Support Manager shall be

responsible for optimizing, standardizing, and improving storage solutions, including facilitating eventual migrations to cloud environments.

It is required that the Infrastructure Support Manager has the following qualifications:

a. Possess a current PMI/PMP certification.
b. A minimum of seven years of experience managing and overseeing operations and projects for infrastructure, systems, and applications at multiple geographically dispersed locations with geographically dispersed teams; similar to the size, scope, and complexity of this TO.
c. Possesses a Top Secret clearance.

It is desired that the Infrastructure Support Manager has the following qualifications:

a. A minimum of three years of experience leading teams that provide full-lifecycle project support, as well as operational support, for Windows and Linux based systems.
b. A minimum of three years of experience leading projects in the MS SQL and Oracle database server environment.
c. A minimum of five years of experience supporting Data Center Operations including supporting/troubleshooting server farms, networking equipment and connections, and storage solutions, (e.g., Cisco Routers and Switches, Firewalls, and Netapp/Dell EMC).

H.1.4 DATABASE SUPPORT MANAGER

The Database Support Manager shall oversee the team responsible for the overall success of the globally dispersed databases. The Database Support Manager shall also be responsible for overseeing the performance of Tier II and Tier III support (as appropriate) in accordance with Section C. This includes supporting Oracle (Version 11g or higher) and Microsoft SQL Server (Version 2008 R2 or higher) platforms and proactively monitoring databases to respond to incidents and alerts. The Database Support Manager shall be responsible for the monitoring and management of the database environment support for CA and for optimizing database performance, availability, and capacity. The Database Support Manager shall also automate manual maintenance, diagnostic health checks, validation, and reporting.

It is required that the Database Support Manager has the following qualifications:

a. Possesses an Oracle Certified Professional (OCP) certification.
b. A minimum of five years of experience in database administration supporting the migration to modernized databases and managing/leading a database staff for projects with a similar size, scope, and complexity to the requirements of the TO.
c. Possesses a CompTIA Security+ certification.
d. Possesses a Top Secret clearance.

It is desired that the Database Support Manager has the following qualifications:

a. Possesses an ITIL Foundations Level Certification (or higher).
b. Demonstrated experience with projecting and planning for long-range requirements for database administration and design.
c. Demonstrated experience conducting quality control and auditing of databases including organization protection and security and documentation and reporting in an environment similar to the CA environment.

d. Demonstrated experience with database technologies, development methodologies, front-end/back-end database programming.

H.1.5 APPLICATIONS SUPPORT MANAGER

The Applications Support Manager shall oversee the team responsible for providing Tier II support to CA/CST IT systems, web applications, unique imaging and archiving applications, client server applications and specialized server applications supporting multiple functions. The Applications Support Manager shall have experience working with Tier III Support.

It is required that the Applications Support Manager has the following qualifications:

a. Possesses an ITIL Foundations Level Certification (or higher).
b. Demonstrated experience with the lifecycle of the SDLC process for applications similar in size, scope, and complexity to the requirements of this TO.
c. A minimum of five years of experience supporting modernized or legacy applications and managing and leading an applications support staff with skills applicable to a project environment, similar in size, scope, and complexity as this TO.
d. Possesses a Secret clearance.

It is desired that the Applications Support Manager has the following qualifications:

a. Possesses a SAFeAgile certification.
b. Possesses a CompTIA Security+ certification.

H.1.6 NETWORK OPERATIONS MANAGER

The Network Operations Manager shall serve as a team leader for support tasks involving engineering development, integration, interface design analysis, integration of infrastructure, and testing of SW and HW. The Network Operations Manager shall perform system-level design and configuration of products including determination of HW, SW, operating systems and other platform specifications to meet project requirements while maintaining interoperability with existing legacy systems. The Network Operations Manager shall plan large-scale systems projects through vendor comparison and trade/cost studies.

It is required that the Network Operations Manager has the following qualifications:

a. A minimum of five years of experience supporting global network systems and subsystems; troubleshooting a wide range of LAN, Multi-Protocol Label Switching (MPLS), WAN, and network/service availability, and making recommendations for system fixes and enhancements.
b. A minimum of five years of experience leading teams of network operations/engineering staff with skills applicable to a project environment similar in size, scope, and complexity to the requirements of this TO.
c. Possesses a Cisco Certified Network Associate (CCNA) certification.
d. Possesses a Top Secret clearance.

It is desired that the Network Operations Manager has the following qualifications:

a. Demonstrated experience with risk management and making recommendations for leveraging network installations and reducing operation costs.
b. Demonstrated experience operating networks supporting systems deployed in the cloud.

c. A minimum of three years working experience supporting and troubleshooting firewall appliances and rulesets and working with firewall solutions such as Palo Alto or Stonegate devices.

H.1.7 ENTERPRISE OPERATIONS CENTER (EOC) MANAGER

The Enterprise Operations Center (EOC) Manager shall be responsible for managing a complex, 24x7x365 enterprise operations center including overseeing an operations team responsible for coordinating and tracking all Tier II incidents (across the enterprise) through resolution. The EOC manager shall be proficient in designing, installing, configuring, maintaining, and operating tools (such as Oracle Enterprise Manager (OEM) Splunk, Solar Winds, VRealize, and Zabbix) to monitor and proactively manage a global IT environment. The EOC manager shall provide monitoring solutions that reduce time, effort, and cost involved with managing and monitoring applications to assess the availability, performance, and capacity for the overall health of the environment.

It is required that the EOC Manager has the following qualifications:

a. Possesses an ITIL Intermediate Level Certification (or higher).
b. A minimum of five years of experience managing an enterprise operations center and managing/ leading enterprise operations center staff with the skills applicable to a project environment similar in size, scope and complexity as this TO.
c. A minimum of five years demonstrated experience triaging and prioritizing critical incidents to directly align with mission objectives.
d. Possesses a Secret clearance.

It is desired that the EOC Manager has the following qualifications:

a. Possesses a CompTIA Security+ certification.

H.1.8 ENGINEERING AND IMPLEMENTATION MANAGER

The Engineering and Implementation Manager is responsible for overseeing and managing all engineering projects and shall provide engineering services for physical and virtual hosting/operating environments for all CA systems, both domestically and abroad. The engineering and design services shall cover physical and virtual Windows and UNIX/Linux Server platforms, as well as Infrastructure-as-a-Service (IaaS) platforms, Platform-as-a-Service (PaaS) offerings, SW-defined infrastructure as cloud service transition within CA. The Engineering and Implementation Manager plays a critical role in the strategic planning of the infrastructure and building a resilient architecture.

It is required that the Engineering and Implementation Manager has the following qualifications:

a. A minimum of five years of experience managing and leading a large engineering and operations staff with skills applicable to a project environment similar in size, scope, and complexity as this TO.
b. Demonstrated experience managing the implementation of technical and process changes in a highly complex infrastructure environment similar to the CA environment, and working collaboratively with internal and external stakeholders such as; the architects, development leads, and operations personnel to gather technical requirements and business needs to design and provision infrastructure capabilities.

c. Demonstrated experience providing leadership for prioritizing, planning, and successfully delivering multiple projects in parallel and in cooperation with a production environment.
d. Experience managing a transition of systems/applications into a cloud environment.
e. Possesses a Top Secret clearance.

It is desired that the Engineering and Implementation Manager has the following qualifications:

a. Demonstrated experience with introducing new technologies and processes to improve service delivery such as availability, management, monitoring, support, patching, and scalability.

H.1.9 ACQUISITION AND ASSET MANAGER

The Acquisition and Asset Manager shall manage the procurement process for all acquisitions obtained by the contractor or the Government. The Acquisition and Asset Manager shall be responsible for managing and tracking accurate inventory of CA/CST assets under this TO. The Acquisition and Asset Manager shall be responsible for supporting bi-annual inventory reviews and for maintaining accurate inventory records. The Acquisition and Asset Manager facilitates renewals of maintenance and support services contracts to ensure availability of post-warranty support and SW upgrade entitlements; resolves warranty disputes and product returns; and identifies and reports market challenges or trends that may prevent timely acquisition of goods and services.
It is required that the Acquisition and Asset Manager has the following qualifications:

a. A minimum of seven years of experience with enterprise IT planning, experience managing inventory and assets, and managing procurements in support of Federal Government clients of similar size, scope, and complexity to this TO.
b. Demonstrated support for lifecycle asset management to include audit response and asset tracking in support of a project of similar size, scope, and complexity to this TO.
c. Demonstrated experience managing and leading an acquisition and asset staff with skills applicable to a project environment similar in size and scope referenced in this TO.

It is desired that the Acquisition and Asset Manager has the following qualifications:

a. Demonstrated experience analyzing organizational IT procurements, identifying opportunities to reduce costs through innovative procurement vehicles, reducing service/support levels to procure necessary support to deliver organizational needs, and analyzing inventory in order to reduce the number of maintenance and support agreements.

H.1.10 SECURITY OPERATIONS MANAGER

The Security Operations Manager shall serve as team leader for operational activities required to maintain the CA production systems security posture in compliance with the DOS' IA and Compliance policies. The Security Operations team is responsible for supporting the Assessment & Authorization (A&A) process in coordination with CA/CST's ISSO team. This includes managing security monitoring, POA&M remediation maintaining standard security configurations in compliance with DOS security standards, managing incident response, supporting security posture assessment and cyber hygiene activities, managing centralized logging and threat analysis, and ensuring consistent, comprehensive and timely patching across the environment.

It is required that the Security Operations Manager has the following qualifications:

a. A minimum of five years of experience with all phases of IA and accreditation processes, securing IT systems and services using Government and industry IA standards, policies, guidelines, and best practices.
b. Demonstrated experience managing and leading a security operations staff with skills applicable to a project environment similar in size and scope referenced in this TO.
c. Demonstrated experience successfully managing information security risks to include completing the entire A&A process including receiving Authority to Operate (ATO) for the cloud.
d. Possesses a Certified Information Systems Security Professional (CISSP) certification.
e. Possesses a Top Secret clearance.

It is desired that the Security Operations Manager Lead has the following qualifications:

a. Demonstrated experience with encryption devices and procedures as they relate to networks and data.

H.1.11 KEY PERSONNEL SUBSTITUTION

The contractor shall not replace any personnel designated as Key Personnel without the written concurrence of the FEDSIM CO. Prior to utilizing other than the Key Personnel specified in its proposal in response to the TOR, the contractor shall notify the FEDSIM CO and the FEDSIM COR of the existing TO. This notification shall be no later than ten calendar days in advance of any proposed substitution and shall include justification (including resume(s) and labor category of proposed substitution(s)) in sufficient detail to permit evaluation of the impact on TO performance.

Substitute Key Personnel qualifications shall be equal to, or greater than, those of the Key Personnel substituted. If the FEDSIM CO and the FEDSIM COR determine that a proposed substitute Key Personnel is unacceptable, or that the reduction of effort would be so substantial as to impair the successful performance of the work under the TO, the contractor may be subject to default action as prescribed by FAR 52.249-6 Termination (Cost Reimbursement).

H.2 GOVERNMENT FURNISHED

H.2.1 GOVERNMENT FURNISHED PROPERTY (GFP)

The GFP will change throughout the life of the TO. The contractor shall maintain a current and historical list of all GFP under this TO. The location of this information will be identified after award. The Government envisions furnishing the contractor with the following equipment:

a. Computer and mobile devices (smart phones) as needed.
b. Passwords and access cards and/or tokens (upon completion of security requirements) to systems and devices required for performance of work.
c. SD toll free number.
d. Furnish the current monitoring and diagnostic tools.
e. HW for on-site functionality. For off-site functionality, CA/CST will provide HW for access to OpenNet and secure networks. This includes Government furnished computers, servers, and other specialized equipment that will be used in conjunction with the OpenNetwork.

f. All HW will be pre-imaged with the required SW including, but not limited to, workstation, operating system, and any SW required for system development and maintenance.

H.2.2 GOVERNMENT FURNISHED SPACE

The Government will provide workspace, as necessary, for individuals assigned to work full time in the DOS facility. The information below represents the open space available within the DOS locations:

a. SA34- Network and Firewall Liaisons- four Seats
b. SA-9 – Network and Firewall Liaison – one Seat
c. BIMC –DATA Center Services—one Seat
d. ESOC West - four Seats
e. SA-17 – 76 Seats
f. Passport Sites/ Domestic Locations --reference **Section J, Attachment K.**

H.3 GOVERNMENT FURNISHED INFORMATION (GFI)

After project start, the Government will provide the GFI listed below including, but not limited to:

a. DOS email accounts
b. Current warranty list for all infrastructure, HW and SW
c. Current license agreements for all SW
d. SOPs
e. KBAs
f. Network topologies
g. SharePoint pages
h. Confluence pages
i. Authenticating and processing Government information on Government resources (e.g., DOS-leased cloud-based systems, OpenNet)
j. Maintenance records for all existing passport card printers

H.4 SECURITY REQUIREMENTS

The association between the contractor and the Government is unclassified; however, disclosure of the TO specifics is on a need-to-know basis. The Government anticipates that work under this TO will be conducted at multiple security levels. Work under this contract will require classified access up to Top Secret (TS).

Under this TO, contractor personnel are required to have a current Secret Personnel Security Clearance (PCLs) and some staff are required to have up to a current Top Secret PCL. The Government will define individual event clearance requirements. Any exceptions must be approved prior to starting work by the FEDSIM Contracting Officer (CO).

The prime contractor and any subcontractors must be able to obtain the required security clearances. The awardee must have the necessary clearances at the time of TOA and throughout the life of the TO. In general, all necessary facility and employee security clearances shall be at the expense of the contractor. The contractor shall comply with all security requirements.

The contractor shall plan for attrition through careful scheduling and advance preparation and submission of clearance requests.

a. A Top Secret Facility Security Clearance (FCL) is required for performance throughout the life of the TO in accordance with the Department of Defense (DD) Form 254, Department of Defense Contract Security Classification Specification (**Section J, Attachment Q**).
b. All contractor personnel assigned to this TO shall possess a Secret or Top Secret PCL issued by the Defense Security Service (DSS) prior to TO performance or billing for time spent on TO tasks.
c. Since it will be necessary for some contractor personnel to have access to classified material and/or to enter into areas requiring a security clearance, each contractor employee requiring such access must have an individual security clearance commensurate with the required access prior to performance. Individuals must maintain their security clearance for the duration of employment under this award.
d. The contractor shall obtain a DOS building pass for all employees performing under this award who require frequent and continuing access to DOS facilities in accordance with DOS Acquisition Regulation (DOSAR) 652.204-70 DOS Personal Identification Card Issuance Procedures.
e. Performance of this TO shall be in accordance with the attached DD Form 254, Department of Defense Contract Security Classification Specification and FAR 52.204-2 "SECURITY REQUIREMENTS".
f. Classified material received or generated in the performance of this award shall be safeguarded and disposed of in accordance with the National Industrial Security Program Operating Manual (NISPOM) (DOD 5220.22 M).
g. To successfully perform under this TO, the contractor, including all entities which comprise a joint venture and the joint venture itself, is required to hold a TOP SECRET FCL issued in accordance with the NISPOM, DoD 5220.22M. Should a party within the joint venture not hold a FCL, the offeror will need to demonstrate that said party will not be performing tasks under the TO which require a clearance (e.g. providing TO required personnel).
h. To demonstrate the existence of a clearance, the offeror shall provide the following:
    1. Narrative confirmation of clearance level. A copy of the National Industrial Security System Facility Verification Notification (NISS FVN) printout is sufficient.
    2. Commercial and Government Entity (CAGE) code.
    3. Complete legal entity name and business address.
i. All building passes/ID cards shall be returned to DOS. Upon completion of this TO, all classified and/or Sensitive But Unclassified (SBU) information shall be returned to the Government.
j. Subcontracting firms must possess FCLs commensurate with their level of access. All subcontractor DD254s shall be prepared and approved by DS/IS/IND prior to performance on this TO.
k. Subsequent to TOA, DOS will conduct a formal briefing for the contractor. The purpose of the briefing will be to bring to the contractor's attention the governing documents and directives regarding all security considerations in the staffing of the project, site access, SW and HW functions, document control, and DS procedures.

l. DOS personnel will provide assistance in obtaining Annex (at 600 19th Street, NW, Washington, D.C.) and work place access during the period of TO support. Contractors must return all access control documentation and building badges to the CA/CST GTM at the completion of TO services.
m. In the event a personnel security clearance is rescinded for an individual assigned to this TO, the individual shall be removed from the TO immediately. The CAEIO contractor shall notify the FEDSIM COR and the CA/CST GTM immediately. In addition, the contractor shall submit a Visit Authorization Request (VAR) cancellation to DS/IS/IND.
n. Security clearance requirements for the contractor to access DOS domestic or overseas information systems shall be in accordance with 12 FAM 600 (reference Web site: http://aope.a.state.gov - click on "FAM" under "References").
o. All personnel who resign, are transferred, terminated, or otherwise removed from the TO on the last day of work on site will be debriefed by the ISSO and shall turn in their DOS badge to the ISSO. The company must cancel the VAR previously sent to DS/IS/IND. Each employee under this TO is individually responsible for the protection of information and shall be required to sign an agreement (DOS Form DS-0109, Separation Statement) regarding the confidentiality of the work performed under this TO.
p. The company FSO must send a VAR to DS/IS/IND via e-mail to ds_ind_contractorvars@state.gov or by facsimile to 571-345-3000. Notification of VAR approvals are provided to the CA/CST GTM.

H.4.1 DOS PERSONAL IDENTIFICATION CARD ISSUANCE PROCEDURES

a. The contractor shall comply with the DOS Personal Identification Card Issuance Procedures for all employees performing under this TO who require frequent and continuing access to DOS facilities or information systems. The contractor shall insert this clause in all subcontracts when the subcontractor's employees will require frequent and continuing access to DOS facilities, or information systems.
b. The DOS Personal Identification Card Issuance procedures may be accessed at http://www.state.gov/m/ds/rls/rpt/c21664.htm.

H.4.2 OPENNET CONNECTIVITY

The contractor will be required to establish connectivity to the Department OpenNet from the contractor site (OpenNet Extension). The program office will sponsor the contractor for the connectivity to OpenNet.

Recent historical data indicates that OpenNet connectivity supporting prior CAEIO activities has previously been supported by network connections with an estimated bandwidth of 110 megabytes (MB). This historical estimated bandwidth does not reflect a recent change in policy that no longer allows remote administration (elevated privileges). This work must be conducted at the Government or contractor site with OpenNet access/drop.

a. The contractor site must be secured for the protection of OpenNet and SBU data. As a minimum, the site must meet the following :
    1. Computer Room - Physical Security.
        i. Perimeter walls must be of slab-to-slab construction to include the area above the false ceiling. #9 10-gauge expanded metal may be used to allow airflow

through openings into the OpenNet space. The barrier must be secured from the OpenNet space.

ii. Openings greater than 96 square inches must be protected by ½" steel bars welded 6" on center vertically and horizontally or with #9 10-gauge expanded metal.

iii. All reverse mounted, out-swinging doors must have heavy-duty butt hinges with non-removable pins.

iv. All reverse mounted, outward-swinging doors must have latch-guard plates installed.

v. All entry points to the suite must be equipped with an Access Control System (ACS) that requires key-card access. Entry and exit audit records must be available for a period of not less than one year.

vi. All monitors must face away from windows or be protected from view by opaque curtains, window shades, or screen-view filters.

vii. There must be an approved shredder available to properly dispose of SBU information. The shredder must meet the requirements of NIST SP 800-88. The shredder must be capable of rendering hardcopy materials unreadable, indecipherable, and irrecoverable.

2. Server Room Configuration.

i. The server room perimeter walls must extend from the structural floor to the structural ceiling.

ii. Openings in the perimeter walls larger than 96 square inches must be screened with 9 gauge expanded metal.

iii. The server room must be located above ground and in interior portions of the building, away from areas subject to frequent use to minimize potential damage from physical and environmental hazards.

iv. The server room must be located away from potential sources of fire such as kitchens, main electrical power distribution panels, and storage areas for combustible materials.

b. Co-location of DOS equipment with personnel that do not possess the minimal security clearance or meet the confirmed 'need to know' requirements to access Department data is prohibited.

c. Personnel (e.g., contractor staff, cleaning staff, building maintenance staff) that do not meet the requirements in paragraphs H.4.b and H.4.c and meet the 'need to know' requirements, but require physical access to areas where the OpenNet equipment is located, must be escorted at all times by a contractor employee that has authorized access to OpenNet.

d. All contractor personnel with access to the OpenNet must report any security incident to the contractor Alternate Information System Security Officer (AISSO), who must report to DS/IS/IND and the contractor Facility Security Officer (FSO) in accordance 12 FAM 590, Cyber Security Incident Program.

e. Contractor personnel must not perform SW development or maintenance on OpenNet.

f. All HW and SW used for this extension must be Local or IT CCB approved and configured, and managed in accordance with 12 FAM 600 and Department security configuration guidelines.

g. All media (e.g., hard drives, compact disks (CDs), flash memory, etc.) used on OpenNet must be returned to CST when:
   1. The media is no longer needed.
   2. The media is inoperative.
   3. The extension is no longer required by the contractor.
   4. The TO is terminated.
h. The OpenNet extension must have no other network connections.
i. All OpenNet processing areas must be approved for the protection of SBU data by DS/IS/IND.
j. The contractor must notify DS/IS/IND when users no longer require access to OpenNet.
k. Any changes to the configuration of this extension (e.g., adding additional workstations, relocating existing workstations) or any changes to the physical structure of the OpenNet space must be approved by DS/SI/CS.
l. DS/IS/IND and the contractor must agree that the OpenNet extension is subject to on-site and remote auditing, scanning, and testing as deemed necessary by DS. This auditing, scanning, and testing will help to assess the compliance of this OpenNet extension with DOS requirements.
m. If at any time, DS finds that the above listed security requirements are not being met, the OpenNet extension will be subject to termination.

H.4.3 WORK AND NETWORK ACCESS DURING TRANSITION-IN

The Transition-In period will allow most technical team members on the incoming TO staff to obtain badges, FOBs, and connect to OpenNet, the Department's non-classified information system.

The Global OpenNet (GO) network, accessed via FOB, provides web-based access to OpenNet and OpenNet-based systems (such as most of the Microsoft Office Suite including Outlook) and will allow some technical work to be done for production support and limited development work via the Electronic Desktop Environment (EDE). However, access to databases for production support is not available through GO; the contractor must have a direct OpenNet connection.

Direct OpenNet connection is provided via a dedicated line or bandwidth and network drops. This requires an inspection of the premises and approval by DS before OpenNet connections can be installed (https://go.state.gov regarding OpenNet.).

Pending a direct OpenNet connection, no technical work will be possible without GO and FOBs. Thus, remote access for teleworking or after hours support via GO will be limited.

H.4.4 INFORMATION ASSURANCE (IA)

The contractor may have access to sensitive (to include privileged and confidential) data, information, and materials of the U.S. Government. These printed and electronic documents are for internal use only and remain the sole property of the U.S. Government. Some of these materials are protected by the Privacy Act of 1974 (AMENDED) and Title 38. Unauthorized disclosure of Privacy Act or Title 38 covered materials is a criminal offense.

H.5 ORGANIZATIONAL CONFLICT OF INTEREST AND NON-DISCLOSURE REQUIREMENTS

H.5.1 ORGANIZATIONAL CONFLICT OF INTEREST (OCI)

a. If a contractor has performed, is currently performing work, or anticipates performing work that creates or represents an actual or potential OCI, the contractor shall immediately disclose this actual or potential OCI to the FEDSIM CO in accordance with FAR Subpart 9.5. The nature of the OCI may involve the prime contractor, subcontractors of any tier, or teaming partners.
b. The contractor is required to complete and sign an OCI Statement (see **Section J, Attachment R).** The contractor must represent either that (1) It is not aware of any facts which create any actual or potential OCI relating to the award of this TO, or (2) It has included information in its proposal, providing all current information bearing on the existence of any actual or potential OCI and has included a mitigation plan in accordance with paragraph (c) below.
c. If the contractor with an actual or potential OCI believes the conflict can be avoided, neutralized, or mitigated, the contractor shall submit a mitigation plan to the Government for review.
d. In addition to the mitigation plan, the FEDSIM CO may require further information from the contractor. The FEDSIM CO will use all information submitted by the contractor, and any other relevant information known to GSA, to determine whether an award to the contractor may take place, and whether the mitigation plan adequately avoids, neutralizes, or mitigates the OCI.
e. If any such conflict of interest is found to exist, the FEDSIM CO may determine that the conflict cannot be avoided, neutralized, mitigated, or otherwise resolved to the satisfaction of the Government, and the contractor may be found ineligible for award. Alternatively, the FEDSIM CO may determine that it is otherwise in the best interest of the U.S. to contract with the contractor and include the appropriate provisions to avoid, neutralize, mitigate, or waive such conflict in the TO awarded.

H.5.2 NON-DISCLOSURE REQUIREMENTS

If the contractor acts on behalf of, or provides advice with respect to any phase of an agency procurement, as defined in FAR 3.104-4, then the contractor shall execute and submit a Corporate Non-Disclosure Agreement (NDA) Form (**Section J, Attachment S)** and ensure that all its personnel (to include subcontractors, teaming partners, and consultants) who will be personally and substantially involved in the performance of the TO:

a. Are instructed in the FAR 3.104 requirements for disclosure, protection, and marking of contractor bid or proposal information, or source selection information.
b. Are instructed in FAR Part 9 for third-party disclosures when acting in an advisory capacity.

All proposed replacement contractor personnel shall also be instructed in the requirements of FAR 3.104. Any information provided by contractors in the performance of this TO or obtained from the Government is only to be used in the performance of the TO. The contractor shall put in place appropriate procedures for the protection of such information and shall be liable to the

Government for any misuse or unauthorized disclosure of such information by its personnel, as defined above.

H.6 SECTION 508 COMPLIANCE REQUIREMENTS

Unless the Government invokes an exemption, all Electronic and Information Technology (EIT) products and services proposed shall fully comply with Section 508 of the Rehabilitation Act of 1973, per the 1998 Amendments, 29 U.S.C. 794d, and the Architectural and Transportation Barriers Compliance Board's Electronic and Information Technology Accessibility Standards at 36 Code of Federal Regulations (CFR) 1194. The contractor shall identify all EIT products and services provided, identify the technical standards applicable to all products and services provided, and state the degree of compliance with the applicable standards. Additionally, the contractor must clearly indicate where the information pertaining to Section 508 compliance can be found (e.g., Vendor's or other exact web page location). The contractor must ensure that the list is easily accessible by typical users beginning at time of award.

H.7 ADEQUATE COST ACCOUNTING SYSTEM

The adequacy of the contractor's accounting system and its associated internal control system, as well as contractor compliance with the Cost Accounting Standards (CAS); affect the quality and validity of the contractor data upon which the Government must rely for its management oversight of the contractor and TO performance. The contractor's cost accounting system shall be adequate during the entire period of performance and shall permit timely development of all necessary cost data in the form required by the Contract.

H.8 APPROVED PURCHASING SYSTEM

The objective of a contractor purchasing system assessment is to confirm it is a Government-approved purchasing system and evaluate the efficiency and effectiveness with which the contractor spends Government funds and complies with Government policy with subcontracting. A Government-audited and approved purchasing system (e.g., approved by DCAA or Defense Contract Management Agency (DCMA)) is mandatory.

When reviews are conducted of the purchasing system during the performance of the TO, the contractor shall provide the results of the review to the FEDSIM CO within ten workdays from the date the results are known to the contractor.

H.9 EARNED VALUE MANAGEMENT (EVM)

The contractor shall employ EVM in the management of this TO in accordance with the American National Standards Institute (ANSI)/Electronic Industries Alliance (EIA) Standard-748-A-1998, *Earned Value Management Systems.* A copy of the standard is available at http://global.ihs.com/. The Government expects the contractor to employ innovation in its proposed application of EVM techniques to this TO in accordance with best industry practices. The following EVM status information shall be included in each CSR:

a. Planned Value (PV)
b. Earned Value (EV)
c. Actual Cost (AC)

d. A cost curve graph plotting PV, EV, and AC on a monthly basis, from inception of the TO through the last report, and plotting the AC curve to the estimated cost at completion (EAC) value.
e. An EVM variance analysis that includes the following:
    1. Cost Variance = (EV - AC)
    2. Cost Variance % = (CV/PV X 100%)
    3. Cost Performance Index (CPI) = (EV/AC)
    4. Schedule Variance = (EV minus PV)
    5. Schedule Variance % = (SV/PV X 100%)
    6. Schedule Performance Index (SPI) = (EV/PV)
    7. Estimate at Completion (EAC)
    8. AC cum + 1/CPI X (BAC minus EV cum)
    9. AC cum + 1/CPI X SPI X (BAC minus EV cum)
    10. Variance at Completion (VAC) = (BAC minus EAC) for EAC
    11. Variance at Completion % + (VAC/BAC X 100%) for EAC
    12. Estimate to Completion (ETC)
    13. Expected Completion Date
f. Explain all variances greater than ten percent
g. Explain, based on work accomplished as of the date of the report, whether the performance goals will be achieved
h. Discuss the corrective actions that will be taken to correct the variances, the risk associated with the actions

The Government will conduct an Integrated Baseline Review after TOA, or exercise of significant TO options, or incorporation of major TO modifications. The contractor shall provide the resulting Integrated Baseline Review documentation to the Government (**Section F, Deliverable 31**). The objective of the Integrated Baseline Review is for the Government and the contractor to jointly assess areas, such as the contractor's planning, to ensure complete coverage of the TO, logical scheduling of the work activities, adequate resources, and identification of inherent risks.

H.10 TRAVEL

H.10.1 TRAVEL REGULATIONS

Contractor costs for travel will be reimbursed at the limits set in the following regulations (see FAR 31.205-46):

a. FTR - prescribed by the GSA, for travel in the contiguous U.S.
b. DSSR (Government Civilians, Foreign Areas), Section 925, "Maximum Travel Per Diem Allowances for Foreign Areas" - prescribed by the DOS, for travel in areas not covered in the FTR or JTR.

H.10.2 TRAVEL AUTHORIZATION REQUESTS (TAR)

Before undertaking long distancetravel to any Government site or any other site in performance of this TO, the contractor shall have this long distance travel approved by, and coordinated with, the FEDSIM COR. Notification shall include, at a minimum, the number of persons in the party, traveler name, destination, duration of stay, purpose, and estimated cost. Prior to any long-

distance travel, the contractor shall prepare a Travel Authorization Request (TAR) (**Section J, Attachment T)** for Government review and approval. Long-distance travel will be reimbursed for cost of travel comparable with the FTR and DSSR for overseas travel. Requests for long distance travel approval shall:

a. Be prepared in a legible manner
b. Include a description of the travel proposed including a statement as to purpose
c. Be summarized by traveler
d. Identify the TO number
e. Identify the CLIN associated with the travel
f. Be submitted in advance of the travel with sufficient time to permit review and approval

The contractor shall use only the minimum number of travelers and rental cars needed to accomplish the task(s). Long distance travel shall be scheduled during normal duty hours whenever possible.

H.11 TOOLS (HARDWARE/SOFTWARE) & ODCS

The Government may require the contractor to purchase HW, SW, and related supplies critical and related to the services being acquired under the TO. Such requirements will be identified at the time a TOR is issued or may be identified during the course of a TO by the Government or the contractor. If the contractor initiates a purchase within the scope of this TO the contractor shall submit to the FEDSIM COR a Request to Initiate Purchase (RIP) **(Section J, Attachment U)**. If the prime contractor is to lose its approved purchasing system, the contractor shall submit to the FEDSIM CO a Consent to Purchase (CTP). The RIP and CTP shall include the purpose, specific items, estimated cost, cost comparison, and rationale. The contractor shall not make any purchases without an approved RIP from the FEDSIM COR or an approved CTP from the FEDSIM CO and without complying with the requirements of Section H.12.

H.12 COMMERCIAL SUPPLIER AGREEMENTS

H.12.1 The Government understands that commercial SW tools that may be purchased in furtherance of this TO as described in **Section C.5.5.1** and as contemplated in the Tools and ODC CLINs in Section **B.4 Services and Prices/Costs** (included with final TO) may be subject to commercial agreements which may take a variety of forms, including without limitation licensing agreements, terms of service, maintenance agreements, and the like, whether existing in hard copy or in an electronic or online format such as “clickwrap” or “browsewrap” (collectively, “Supplier Agreements”). For purposes of this TO, the Supplier Agreements are “collateral agreements” within the meaning of the FAR clause at 52.227-14.

H.12.2 The contractor shall ensure that any proposed Supplier Agreements allow the associated SW and services to be used as necessary to achieve the objectives of this TO. The contractor shall provide all applicable Supplier Agreements to the FEDSIM CO prior to purchase and shall cooperate with the Government, including negotiations with the licensor as appropriate, to ensure compliance with this Section. Without limiting the generality of the foregoing, a compliant Supplier Agreement shall permit all of the following at no extra charge to the Government: (a) access and use by support contractors, including a successor contractor upon termination or expiration of this TO; (b) access and use by employees of other Federal, state, and local law enforcement agencies; (c) transfer to a different data center and/or a successor contractor’s cloud; and (d) the creation of derivative works that shall be subject to at least the same rights as

set forth in subparagraphs (a) through (c) above. The above rights constitute "other rights and limitations" as contemplated in subparagraph (d) of the FAR clause at 52.227-14, Rights In Data – General (May 2014), Alternate III (Dec 2007).

H.13 PRESS RELEASE

The contractor shall not make any press/news release pertaining to this procurement without prior Government approval and only in coordination with the FEDSIM CO.

H.14 INTELLECTUAL PROPERTY RIGHTS

The existence of any patent, patent application or other intellectual property right that encumbers any deliverable must be disclosed in writing on the cover letter that accompanies the delivery. If no such disclosures are provided, the data rights provisions in FAR 52.227-14 apply.

H.15 AWARD FEE

See the AFDP in **Section J, Attachment C.**

H.16 TELEWORK

Telework is not a requirement for this TO; however, telework can be performed on a case-by-case basis. The contractor shall adhere to DOS and CA/CST telework policy and procedures. Contractor employees approved for telework will follow current State Department policies and procedures to access DOS OpenNet systems remotely using Department approved remote access methods. Any contractors performing functions requiring elevated privileges while teleworking will require additional approvals and must follow all DOS and CA/CST policies and procedures for remote access with elevated privileges. The contractor must request and receive approval of their telework plan prior to performing telework. Contractors must be signed into the Department standard collaboration tool (i.e., TEAMS) while teleworking, and must be responsive to official contacts via the collaboration tool.

H.17 CARES ACT SECTION 3610 COST REIMBURSEMENT

Prior to submitting an invoice for reimbursement of paid leave costs pertaining to Section 3610 of the CARES Act, the contractor shall submit estimates for the upcoming invoice period to the FEDSIM COR and TPOC. Any estimates shall be between January 31, 2020 and March 31, 2021. The estimates shall include, at a minimum, the invoice period, names, hours, minimum billing rate, and associated costs for applicable personnel. The contractor's estimate shall include anticipated invoice reductions for all credits or relief to which the contractor may be entitled pursuant to division G of the Families First Coronavirus Response Act (Pub. L. 116–127) and any applicable relief to which the contractor may be entitled under the CARES Act (Pub. L. 116-136) or any other relief allowed by the laws of any jurisdiction to which the contractor may be entitled that is specifically identifiable with the public health emergency declared on January 31, 2020 for COVID–19. This requirement applies regardless of whether the contractor is in actual receipt of or has properly effectuated the accrual of such other relief in its accounting systems, or has properly pursued such relief at the time of estimate submission. The contractor shall submit the estimate utilizing the attachment provided in Section J, Attachment AM (CARES ACT Reimbursement Request). Submission of an estimate does not constitute prior authorization. The contractor shall follow all invoice requirements.

I.1 TASK ORDER CLAUSES

All applicable and required clauses set forth in FAR 52.301 automatically flow down to all Alliant 2 TOs, based on their specific contract type (e.g., cost, fixed-price, etc.), statement of work, competition requirements, commercial or not commercial, and dollar value as of the date the TO solicitation is issued.

I.2 FAR 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

This TO incorporates one or more clauses by reference with the same force and effect as if they were given in full text. Upon request, the FEDSIM CO will make their full text available. Also, the full text of a clause may be accessed electronically at the FAR website:

http://www.acquisition.gov/far/

FAR	TITLE	DATE
52.203-13	Contractor Code of Business Ethics and Conduct	OCT 2016
52.203-14	Display of Hotline Poster(s) https://www.stateoig.gov/system/files/hotlineposter_stateoig.pdf	OCT 2016
52.203-17	Contractor Employee Whistleblower Rights and Requirement to Inform Employees of Whistleblower Rights	APR 2014
52.204-2	Security Requirements	AUG 1996
52.204-9	Personal Identity Verification of Contractor Personnel	JAN 2011
52.204-10	Reporting Executive Compensation and First-Tier Subcontract Awards	OCT 2016
52.204-13	System for Award Management Maintenance	OCT 2016
52.204-14	Service Contract Reporting Requirements	OCT 2016
52.204-18	Commercial and Government Entity Code Maintenance	AUG 2020
52.204-21	Basic Safeguarding of Covered Contractor Information Systems	JUN 2016
52.204-23	Prohibition On Contracting For Hardware, Software, and Services Developed or Provided By Kaspersky Lab And Other Covered Entities	JUL 2018
52.215-21	Requirements for Certified Cost or Pricing Data and Data Other than Certified Cost or Pricing Data—Modifications	OCT 2010
52.215-23	Limitations on Pass-Through Charges	OCT 2009
52.216-7	Allowable Cost and Payment Fill-in: 30 Days	AUG 2018
52.219-8	Utilization of Small Business Concerns	NOV 2016
52.222-2	Payment for Overtime Premiums Fill-in: $308,328	JUL 1990
52.223-15	Energy Efficiency in Energy Consuming Products	DEC 2007
52.223-16	Acquisition of EPEAT®-Registered Personal Computer Products	OCT 2015

FAR	TITLE	DATE
52.224-1	Privacy Act Notification	APR 1984
52.224-2	Privacy Act	APR 1984
52.225-13	Restrictions on Certain Foreign Purchases	JUN 2008
52.227-14	Rights in Data – General	MAY 2014
52.227-14	Rights In Data—Alternate III	DEC 2007
52.227-17	Rights In Data Special Works	DEC 2007
52.232-18	Availability of Funds	APR 1984
52.232-20	Limitation of Cost	APR 1984
52.232-22	Limitation of Funds	APR 1984
52.232-40	Providing Accelerated Payments to Small Business Subcontractors	DEC 2013
52.234-4	Earned Value Management System	May 2014
52.237-3	Continuity of Services	JAN 1991
52.239-1	Privacy or Security Safeguards	AUG 1996
52.244-6	Subcontracts for Commercial Items	JAN 2017
52.245-1	Government Property	JAN 2017
52.246-5	Inspection of Services—Cost-Reimbursement	APR 1984
52.246-11	Higher-Level Contract Quality Requirement	DEC 2014
52.246-25	Limitation of Liability – Services	FEB 1997
52.247-67	Submission of Transportation Documents for Audit Fill-in: COR, see Section G	FEB 2006
52.249-6	Termination (Cost-Reimbursement)	MAY 2004
52.249-14	Excusable Delays	APR 1984
52.251-1	Government Supply Sources	APR 2012

I.2.1 FAR CLAUSES INCORPORATED BY FULL TEXT

FAR 52.204-25 PROHIBITION ON CONTRACTING FOR CERTAIN TELECOMMUNICATIONS AN VIDEO SURVEILLANCE SERVICES OR EQUIPMENT (AUG 2020)

(a) *Definitions.* As used in this clause—

Backhaul means intermediate links between the core network, or backbone network, and the small subnetworks at the edge of the network (*e.g.*, connecting cell phones/towers to the core telephone network). Backhaul can be wireless (e.g., microwave) or wired (*e.g.*, fiber optic, coaxial cable, Ethernet).

Covered foreign country means The People's Republic of China.

Covered telecommunications equipment or services means–

(1) Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities);

(2) For the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities);

(3) Telecommunications or video surveillance services provided by such entities or using such equipment; or

(4) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

Critical technology means–

(1) Defense articles or defense services included on the United States Munitions List set forth in the International Traffic in Arms Regulations under subchapter M of chapter I of title 22, Code of Federal Regulations;

(2) Items included on the Commerce Control List set forth in Supplement No. 1 to part 774 of the Export Administration Regulations under subchapter C of chapter VII of title 15, Code of Federal Regulations, and controlled-

(i) Pursuant to multilateral regimes, including for reasons relating to national security, chemical and biological weapons proliferation, nuclear nonproliferation, or missile technology; or

(ii) For reasons relating to regional stability or surreptitious listening;

(3) Specially designed and prepared nuclear equipment, parts and components, materials, software, and technology covered by part 810 of title 10, Code of Federal Regulations (relating to assistance to foreign atomic energy activities);

(4) Nuclear facilities, equipment, and material covered by part 110 of title 10, Code of Federal Regulations (relating to export and import of nuclear equipment and material);

(5) Select agents and toxins covered by part 331 of title 7, Code of Federal Regulations, part 121 of title 9 of such Code, or part 73 of title 42 of such Code; or

(6) Emerging and foundational technologies controlled pursuant to section 1758 of the Export Control Reform Act of 2018 (50 U.S.C. 4817).

Interconnection arrangements means arrangements governing the physical connection of two or more networks to allow the use of another's network to hand off traffic where it is ultimately delivered (*e.g.*, connection of a customer of telephone provider A to a customer of telephone company B) or sharing data and other information resources.

Reasonable inquiry means an inquiry designed to uncover any information in the entity's possession about the identity of the producer or provider of covered telecommunications equipment or services used by the entity that excludes the need to include an internal or third-party audit.

Roaming means cellular communications services (*e.g.*, voice, video, data) received from a visited network when unable to connect to the facilities of the home network either because signal coverage is too weak or because traffic is too high.

Substantial or essential component means any component necessary for the proper function or performance of a piece of equipment, system, or service.

(b) *Prohibition*.

(1) Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. The Contractor is prohibited from providing to the Government any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104.

(2) Section 889(a)(1)(B) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2020, from entering into a contract, or extending or renewing a contract, with an entity that

uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104. This prohibition applies to the use of covered telecommunications equipment or services, regardless of whether that use is in performance of work under a Federal contract.

(c) *Exceptions.* This clause does not prohibit contractors from providing—

(1) A service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(2) Telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(d) Reporting requirement.

(1) In the event the Contractor identifies covered telecommunications equipment or services used as a substantial or essential component of any system, or as critical technology as part of any system, during contract performance, or the Contractor is notified of such by a subcontractor at any tier or by any other source, the Contractor shall report the information in paragraph (d)(2) of this clause to the Contracting Officer, unless elsewhere in this contract are established procedures for reporting the information; in the case of the Department of Defense, the Contractor shall report to the website at https://dibnet.dod.mil. For indefinite delivery contracts, the Contractor shall report to the Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided at https://dibnet.dod.mil.

(2) The Contractor shall report the following information pursuant to paragraph (d)(1) of this clause

(i) Within one business day from the date of such identification or notification: the contract number; the order number(s), if applicable; supplier name; supplier unique entity identifier (if known); supplier Commercial and Government Entity (CAGE) code (if known); brand; model number (original equipment manufacturer number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

(ii) Within 10 business days of submitting the information in paragraph (d)(2)(i) of this clause: any further available information about mitigation actions undertaken or recommended. In addition, the Contractor shall describe the efforts it undertook to prevent use or submission of covered telecommunications equipment or services, and any additional efforts that will be incorporated to prevent future use or submission of covered telecommunications equipment or services.

(e) *Subcontracts.* The Contractor shall insert the substance of this clause, including this paragraph (e) and excluding paragraph (b)(2), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items.

(End of clause)

FAR 52.217-8 OPTION TO EXTEND SERVICES (NOV 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed six months. The Contracting Officer may exercise the option by written notice to the Contractor within 30 Days.

(End of clause)

FAR 52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000)

a. The Government may extend the term of this contract by written notice to the Contractor within 30 days; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 60 days before the contract expires. The preliminary notice does not commit the Government to an extension.
b. If the Government exercises this option, the extended contract shall be considered to include this option clause.
c. The total duration of this contract, including the exercise of any options under this clause, shall not exceed ninety months.

(End of clause)

I.3 GENERAL SERVICES ADMINISTRATION ACQUISITION MANUAL (GSAM), CLAUSES INCORPORATED BY REFERENCE

The full text of a clause may be accessed electronically at the GSAM website:

https://www.acquisition.gov/gsam/gsam.html/

GSAM	TITLE	DATE
552.204-9	Personal Identity Verification Requirements	OCT 2012
552.232-25	Prompt Payment	NOV 2009
552.232-39	Unenforceability of Unauthorized Obligations (FAR Deviation)	FEB 2018
552.232-78	Commercial Supplier Agreements Unenforceable Clauses	FEB 2018

I.3.1 GSAM CLAUSES INCORPORATED BY FULL TEXT

GSAM 552.212-71 CONTRACT TERMS AND CONDITIONS APPLICABLE TO GSA ACQUISITION OF COMMERCIAL ITEMS (JUNE 2016)

(a) The Contractor agrees to comply with any clause that is incorporated herein by reference to implement agency policy applicable to acquisition of commercial items or components. The clause in effect based on the applicable regulation cited on the date the solicitation is issued applies unless otherwise stated herein. The clauses in paragraph (b) of this section are incorporated by reference:

(b) Clauses.

552.203-71 Restriction on Advertising

552.215-70 Examination of Records by GSA

(End of clause)

GSAM 552.222-70 CARES ACT SEC. 3610 PAID LEAVE REIMBURSEMENTS (APR 2020)

(a) Definitions:

(1) Affected contractor: shall mean a contractor under a services contract or a construction contract, whose employees or subcontractors cannot perform work on a site that has been approved by the Government (including a Federally-owned or leased facility or site) due to facility closures or other restrictions and who cannot telework because their job duties cannot be performed remotely during the COVID-19 public health emergency (which was declared on January 31, 2020), from March 27, 2020, through March 31, 2021.

(2) Applicable rate: shall mean the lowest contract billing rate for the specific applicable work categories for which reimbursement is requested.

(3) Applicable work: shall mean work that an affected contractor (or its subcontractors) cannot perform on a site that has been approved by the Federal Government (including a Federally-owned or leased facility or site) due to facility closures or other restrictions and who cannot telework because their job duties cannot be performed remotely during the COVID-19 public health emergency (which was declared on January 31, 2020) from March 27, 2020, through March 31, 2021, and such work cannot be performed using telework or other remote means.

(4) Reimbursable leave: shall mean any paid leave, including sick leave, which an affected contractor provides during the period of March 27, 2020, through March 31, 2021, to keep its employees or subcontractors in a ready state. For affected contractors or their subcontractors, reimbursable leave shall not exceed an average of 40 hours per week.

(5) Covered credits: shall mean the amount of any credit received by an affected contractor pursuant to any section of the Coronavirus Aid, Relief, and Economic

Security (CARES) Act of 2020 or division G of the Families First Coronavirus Response Act of 2020.

(b) Authority: Section 3610 of the CARES Act, Public Law 116-136, states that notwithstanding any other provision of law, and subject to the availability of appropriations, funds made available to an agency by this Act or any other Act may be used by such agency to modify the terms and conditions of a contract, or other agreement, without consideration, to reimburse at the minimum applicable contract billing rates not to exceed an average of 40 hours per week any paid leave, including sick leave, a contractor provides to keep its employees or subcontractors in a ready state, including to protect the life and safety of Government and contractor personnel, but in no event beyond March 31, 2021. Such authority shall apply only to a contractor whose employees or subcontractors cannot perform work on a site that has been approved by the Federal Government, including a federally-owned or leased facility or site, due to facility closures or other restrictions, and who cannot telework because their job duties cannot be performed remotely during the public health emergency (declared on January 31, 2020) for COVID-19: Provided, that the maximum reimbursement authorized by this section shall be reduced by the amount of credit a contractor is allowed pursuant to division G of Public Law 116-127 and any applicable credits a contractor is allowed under the CARES Act.

(c) General rule: An affected contractor may request an equitable adjustment for, and the Government may reimburse, reimbursable leave paid by the affected contractor for leave during the period of March 27, 2020, through March 31, 2021. Such reimbursements shall only cover actual reimbursable leave paid by the affected prime contractor, including payments to a subcontractor to cover paid leave paid to subcontractor's employees. Where practicable, it shall not include profit or fees. It shall not exceed the applicable rate. Whether to reimburse, and how much to reimburse, are at the sole and absolute discretion of the Government.

(d) Time of reimbursement: The Contractor may submit the request for reimbursement immediately after making the payment to the Contractor's employee(s), or making the payment to the subcontractor that has already made the payment to the subcontractor's employee(s). The submission is allowed notwithstanding restrictions in an interim payment clause or advance payment clause in this contract, and no advance payment bond or other security or lien is required for the reimbursement.

(e) Request:

(1) Any affected contractor requesting reimbursement shall provide any documentation requested by the Contracting Officer. At a minimum the documentation must contain:

(i) A representation by the affected contractor that—

(A) The reimbursement request for paid leave is only for reimbursable leave for applicable work, at the applicable rate in accordance with clause 552.222-70.

(B) If the contractor receives covered credits, the contractor will timely notify the contracting officer of the circumstances of receiving the covered credits (e.g., dates and amounts).

(C) All information submitted is true, accurate, complete, and correct as of the date of its submission to the Contracting Officer.

(ii) The total estimated amount the contractor expects to request for reimbursable leave.

(2) The affected contractor shall provide a representation in accordance with paragraph (e)(1)(i) for all requests for reimbursement.

(3) Any affected contractor shall maintain records of the documentation supporting their request, including those requested by the Contracting Officer, in an auditable format, for three (3) years after final payment on the contract.

(4) The Contracting Officer, or an authorized representative of the Contracting Officer, including an Inspector General, the Comptroller General (under Section 19010 of the CARES Act), and the Pandemic Response Accountability Committee (under Section 15010 of the CARES Act), shall have the right to examine and audit all the pertinent records and affected contractor employees.

(f) Repayment: The affected contractor is not allowed to keep any double reimbursements after the application of covered credits. Therefore, if the affected contractor receives covered credits then the Contractor shall notify the Contracting Officer, in writing. The Contractor shall repay the Government the amount of the reimbursement up to the amount of the covered credits. The amount of repayment owed to the Government is considered an overpayment. See Federal Acquisition Regulation 3.1003(a)(3).

(g) Work sites: All contractor and subcontractor work sites are considered approved for purposes of this clause, except for work sites which the Contracting Officer identifies specifically in writing as not approved.

(End of Clause)

I.4 HOMELAND SECURITY PRESIDENTIAL DIRECTIVE 12 (HSPD-12) AND DOS ACQUISITION REGULATION (DOSAR) 652.204-70

The contractor shall comply with the DOS Personal Identification Card Issuance Procedures for all employees performing under this contract who require frequent and continuing access to DOS facilities or information systems.

Homeland Security Presidential Directive 12 (HSPD-12) requires Federal agencies to develop and deploy for their contract personnel and employees a Personal Identity Verification (PIV) credential that is secure, reliable, and interoperable among all Federal agencies (NIST 800-116).

HSPD-12 mandates the establishment of a Government-wide standard for identity credentials to improve physical security in Federally controlled facilities. To that end, HSPD-12 requires all Government employees and contractors be issued a new identity credential based on the Federal Information Processing Standard Publication (FIPS) 201 on PIV. FIPS 201 is a U.S. Federal Government standard that specifies PIV requirements for Federal employees and contractors. Following FIPS 201, this credential is referred to herein as a PIV Card.

HSPD-12 explicitly requires the use of PIV Cards "in gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems." In response to HSPD-12, the NIST Computer Security Division initiated a new program for improving the identification and authentication of Federal employees and contractors for access to Federal facilities and information systems. FIPS 201 was developed to satisfy the technical requirements of HSPD-12, approved by the Secretary of Commerce, and issued on February 25, 2005.

All contractor personnel shall meet a minimum vetting standard and an ID must be issued for physical and logical access.

References:

a. http://www.state.gov/m/ds/rls/rpt/c21664.htm
b. HSPD-12
c. FIPS 201-2
d. NIST SPs

The DOS Personal Identification Card Issuance Procedures may be accessed at: http://www.state.gov/m/ds/rls/rpt/c21664.htm

J.1 LIST OF ATTACHMENTS

The following attachments are attached, either in full text or electronically at the end of the TOR.

ATTACHMENT	TITLE
A	Acronym List
B	Incremental Funding Chart (electronically attached .xls)
C	Award Fee Determination Plan (AFDP3)-Mod 10
D	Reserved
E	Contract Status Report (CSR) Template
F	Weekly Activity Report (WAR) and Project Status Report (PSR) Template
G	Reserved
H	Reserved
I	Reserved
J	Trip Report Template
K	Reserved
L	Reserved
M	Reserved
N	Deliverable Acceptance-Rejection Report Template
O	Problem Notification Report (PNR)
P	COR Appointment Letter
Q	Department of Defense (DD) 254 47QFCA-19-R-0023 (electronically attached .pdf)
R	Organizational Conflict of Interest (OCI) Statement
S	Corporate Non-Disclosure Agreement (NDA)
T	Travel Authorization Request (TAR) Template (electronically attached .xls)
U	Request to Initiate Purchase (RIP) Template (electronically attached .xls)
V	Reserved
W	Reserved
X	Reserved
Y	Service Level Agreements (SLAs) – Mod 08
Z	Reserved
AA	Reserved
AB	Reserved
AC	Reserved
AD	Reserved
AE	Reserved
AF	Reserved
AG	Reserved
AH	Reserved
AI	Reserved
AJ	Reserved

ATTACHMENT	TITLE
AK	Alternate COR Designation Letter
AL	FAR Provision 52.204-24 Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment
AM	CARES ACT Reimbursement Request